1999-03

Data integrity in RFID systems

Alchazidis, Nikolaos.

Monterey California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DATA INTEGRITY IN RFID SYSTEMS

by

Nikolaos Alchazidis

September 2006

Thesis Advisor:	Weilian Su
Co- Advisor:	Tri T. Ha

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE | *Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE**	**3. REPORT TYPE AND DATES COVERED**
	September 2006	Master's Thesis

4. TITLE AND SUBTITLE: Data Integrity in RFID Systems

5. FUNDING NUMBERS

6. AUTHOR(S) Nikolaos Alchazidis

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

One of the main problems that affect the data integrity of passive RFID systems is the collision between the tags. A popular anticollision algorithm which dominates the standards in HF and UHF passive RFID systems is Framed Slotted Aloha (FSA) and some variations of FSA. Throughput and Average time delay of the RFID system which determines the performance/efficiency of the system are reduced rapidly when the number of tags inside the interrogation zone is increased. Using larger frame sizes is not always the solution. This thesis discusses and compares the existing protocols, and proposes a variation of FSA, called Progressing Scanning (PS) algorithm. The PS algorithm divides the tags in the interrogation zone into smaller groups, and gives the ability to the reader to communicate each time with one of them. For performance analysis, the PS algorithm was evaluated with the parameters of a typical passive RFID system at $2.45\,GHz$. The results showed that the PS algorithm can improve the efficiency of the RFID system and provide a reliable solution for cases with a high density of tags in the area (over $800\,tags$).

14. SUBJECT TERMS Passive RFID Systems, Tags, Framed Slotted Aloha (FSA), Collisions, Data Integrity, Progressing Scanning (PS) Algorithm.

15. NUMBER OF PAGES
113

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

DATA INTEGRITY IN RFID SYSTEMS

Nikolaos Alchazidis
Lieutenant, Hellenic Navy
B.S., Hellenic Naval Academy, 1996

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTICAL ENGINEERING
and
MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2006

Author: Alchazidis Nikolaos

Approved by: Weilian Su
Thesis Advisor

Tri T. Ha
Co- Advisor

Jeffrey B. Knorr
Chairman, Department of Electrical and Computer Engineering

Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

One of the main problems that affect the data integrity of passive RFID systems is the collision between the tags. A popular anticollision algorithm which dominates the standards in HF and UHF passive RFID systems is Framed Slotted Aloha (FSA) and some variations of FSA. Throughput and Average time delay of the RFID system which determines the performance/efficiency of the system are reduced rapidly when the number of tags inside the interrogation zone is increased. Using larger frame sizes is not always the solution. This thesis discusses and compares the existing protocols, and proposes a variation of FSA, called Progressing Scanning (PS) algorithm. The PS algorithm divides the tags in the interrogation zone into smaller groups, and gives the ability to the reader to communicate each time with one of them. For performance analysis, the PS algorithm was evaluated with the parameters of a typical passive RFID system at $2.45\,GHz$. The results showed that the PS algorithm can improve the efficiency of the RFID system and provide a reliable solution for cases with a high density of tags in the area (over $800\,tags$).

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This work is dedicated to the memory of my lovely brother Georgios and my father Vasileios, who were a source of inspiration in every step of my life. I also dedicate this thesis to my mother Anastasia; my thoughts will always be with her, no matter how faraway I will be.

First, I would like to acknowledge the support I received from my lovely wife Antigoni at home during my efforts to write this thesis, my daughter Vasiliki and my son Anastasios-Orfeas for their patience during this time. I am very grateful for the time they let me spend away from them.

Furthermore, I would like to express my appreciation to my thesis advisor Professor Weilian Su for his guidance and useful remarks about my work, especially during the development of the proposed algorithm, and also my thesis co-advisor Professor Tri Ha for his wise and very accurate remarks about the communication part of my thesis. I would also like to thank Nancy Sharrock for her help in editing and formatting my thesis.

Last but not least, I would like to thank Bob Broadston, the lab director of the microwave lab for his assistance and truly useful tips in writing my Matlab code for the simulation of the proposed algorithm.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

A huge revolution has occurred in Radio Frequency Identification (RFID) systems during the past decades. More vendors are involved and have invested in this technology, which promises wholesale changes across a broad spectrum of business activities. The Department of Defense (DoD), Wal-Mart , and other large organizations require suppliers to implement RFID technology in their products with the goal of decreasing costs and reducing order cycle times so as to achieve automatic replenishment and enhance collaboration between suppliers and customers. For the above reasons, RFID tags have already been substituted for barcodes in many implementations such as the tracking of baggage in many airports.

Currently, RFID systems are usually available in low, high, ultra-high, and microwave frequencies with passive, semi-passive (or semi-active) and active transponders or *Tags*. Tags might be either Chipless, or contain a microchip with read only, or read and write memory. The component controlling communication in a RFID system is called a *Reader* or interrogator, which can be stationary or portable depending on the application. In order for the tags to transmit their data, the tags must be in the reader's field or interrogation zone, and receive the necessary energy from the reader. This thesis is interested in passive microwave (at $2.45\,GHz$) RFID systems using tags with read-only capabilities.

Communication between the reader and tags in the reverse channel (tags to reader) is a multiuser environment where the main problem is collision because more than one tag transmits to the reader at the same time and frequency. Collision affects the data integrity of the RFID system, and degrades performance.

Two main anticollision protocols dominate the standards established either by the Electronic Product Code (EPC), which was developed at M.I.T, or by the International Organization for Standardization (ISO), Aloha based protocols that are probabilistic and binary tree based that can be either probabilistic or deterministic. This thesis investigates

the probabilistic protocols and especially the Framed Slotted Aloha (FSA) algorithm, which is the most common and also simplest variation of the Aloha algorithm currently used in passive RFID systems.

The objectives of this thesis are as follows:

- To discuss and investigate if the existing anticollision protocols in passive RFID systems can be improved.
- To compare the existing probabilistic anticollision protocols.
- To propose an anticollision protocol capable of providing a high level of data integrity in passive RFID systems at $2.45\,GHz$. This protocol must be simple and also able to handle a RFID system with a large number of tags.
- To discuss additional techniques to improve data integrity in a typical RFID system, and finally
- To propose applications where a passive microwave RFID system with the proposed protocol can be used.

Passive RFID systems have many limitations compared to other wireless communications systems. The tags, which use the reverse channel, are powerless and stateless devices that cannot communicate with each other, and in general, have few capabilities. They can only receive commands from the reader, and therefore, do not have the ability to sense the medium and detect a collision. As a result, the anticollision protocol must be simple enough to implement to lead to low efficiency.

FSA is the simplest probabilistic anticollision algorithm that can be used with a maximum theoretical throughput of $36.8\,\%$. All the variations of FSA currently proposed in literature cannot increase this limit. They can only succeed in operating near this limit, providing stability to the RFID system, and thus increasing the performance in terms of average time delay.

Two main variations of FSA increase the performance of passive RFID systems. The first is called *Dynamic Framed Slotted Aloha* (DFSA). In DFSA, the reader needs to estimate the number of tags in the interrogation zone, and in the next transmission, use a frame size equal to this number. The authors of DFSA demonstrated in their simulations using OPNET that DFSA, compared to the conventional FSA, performs better regardless of the number of tags in terms of identification time. The maximum number of tags used

in their simulations was 900. A comparison of DFSA with FSA in this thesis shows that theoretical DFSA improves the performance in terms of identification time, and also provides a more stable communication link because throughput is almost constant and equal to the maximum theoretical value of 36.8% in DFSA. The only problem addressed by DFSA is that, in reality, it might not be easy and cost effective for vendors to manufacture a reader with the capability of estimating the number of tags, and use a variable frame size. Also, another concern is a possible physical limitation in increasing the frame size.

The second is called *Enhanced Dynamic Framed Slotted Aloha* (EDFSA). EDFSA promises to provide a solution to the above limitation of DFSA. In this variation of FSA, the reader needs again to estimate the number of unread tags in the interrogation zone. In next transmission, the reader either adjusts the frame size to the optimal one as in DFSA or adjusts the number of tags that will respond to reader signals. This second approach is very effective when the number of tags is too high. EDFSA increases the performance of the RFID system and outperforms FSA and DFSA. However, it needs a more complicated reader to perform the above calculations, and also, in order to divide the tags into smaller groups, more signals/commands are necessary to send to the tags. Therefore, the complexity of the tags and the manufacturing cost increases.

This thesis proposes a new anticollision protocol, a variation of FSA called the *Progressing Scanning* (PS) algorithm, which is capable of dividing the number of tags into smaller groups such as the EDFSA protocol. However, the PS algorithm is based on simplicity for both the tags and the reader. It can also take into account an estimation of the number of tags, and thus, improve performance, but this goes against the main principle of having a very simple and cost effective system.

In the PS algorithm, the reader takes advantage of the range difference between the tags and the reader's antenna. Tags near the reader receive more power from the reader than those further away. Therefore, the PS algorithm divides the number of tags n in the area into smaller groups as in the EDFSA algorithm.

This thesis implements the PS algorithm in a passive RFID system at $2.45\,GHz$, and based on the parameters given in ISO/IEC 18000-4 standards, simulates this system using Matlab. The comparison between the FSA and PS algorithm demonstrated that the PS algorithm can improve the efficiency of the RFID system and provide a reliable solution for cases with a high density of tags in the area (over $800\,tags$).

Comparing PS algorithm with DFSA would be not appropriated since the authors of DFSA use a different frame structure and simulation approach in their research. Also in the EDFSA algorithm, the authors use quite different parameters to evaluate the performance of their work, and as a result, the PS algorithm was only compared to FSA.

The parameters that control the performance of the proposed algorithm are the selected frame size, the minimum reader's transmitted power, the number of tags inside the interrogation zone, and finally, the *step* used to increase the transmitted power in each new cycle. If the number of tags is known, the frame size and the step size can be selected and improve the performance of the system. On the other hand, if it is unknown, the PS algorithm can use small frame sizes and handle the collision between tags while FSA cannot.

Furthermore, this thesis discusses other parameters that can affect data integrity in RFID systems, such as the capture effect and the length of tags messages. Use of the capture effect can increase the maximum theoretical throughput up to $46\,\%$ for a typical RFID system. Also, the length of the frame that tags are using for their response should be as small as possible in order to decrease the probability of frame error. The optimal frame length was set equal to $96\,bits$, and this number was used in the calculation of the average time delay of the system.

Finally, this thesis proposes the use of a semi-passive microwave RFID system with protocol compatible with IEEE 802.11 and IEEE 802.15 for power efficiency and also to identify and track friendly forces.

I. INTRODUCTION

A. PURPOSE OF RADIO FREQUENCY IDENTIFICATION TECHNOLOGY (RFID)

Currently, a revolution is occurring in Radio Frequency Identification (RFID) technology, and many companies create new implementations of RFID systems and new products related to this technology daily.

The main advantage of RFID technology is the automated identification and data capture that promises wholesale changes across a broad spectrum of business activities and aims to reduce the cost of the already used systems such as barcodes. For this reason, although RFID technology was discovered many years ago, it has advanced and evolved only during the last decade since cost has been the main limitation in all implementations.

The main advantages of RFID systems compared to barcodes are the following:

- In RFID applications intended to replace barcodes, contact with the item to be identified is not necessary, and even the line-of-sight is often not necessary. Thus, it is no longer necessary to open shipping boxes and scan their contents.
- RFID systems work over long distances.
- RFID provides full automation of the supply chain and can reduce the cost of the vendor using it.
- It can be implemented in different environmental conditions, such as in rain or with dust and dirt and still operate extremely well.
- Also, while data stored in barcodes are fixed and cannot be changed, in most RFID systems, this is possible by changing the data inside their electronic memory.
- RFID systems are capable of multiple simultaneous scans of items which reduce the time needed to collect the data.
- RFID systems can be used to track people and animals in real time, while this cannot be done with barcodes.
- A barcode is the same for all similar items, while with RFID technology, the same items can have different data, such as a different expiration date.

A disadvantage of RFID technology is that the manufacturing cost of the main components is still not cheaper than simple barcodes. Therefore, barcodes will coexist with RFID systems in some applications.

Due to the relative high data rates and the long tracking distance, RFID systems are being examined to ascertain whether they could be employed for tracking people and supplies in military operations. The most important issues to be solved are the integrity of data collection and the security of data transferred in the RFID system. In general, RFID technology has vulnerabilities in securing the data between the main components of the RFID system.

B. SCOPE OF THESIS

This thesis proposes to investigate RFID technology and evaluate the performance/effectiveness of the RFID systems in collecting data. It intends to discuss and evaluate the performance of the different protocols used today for communication between the main components of the RFID system: the *tags* and the *reader*.

It focuses on RFID systems which work in the microwave frequency band of 2.45 GHz, without the use of a battery supply for the tags. The goal of this research is to discover ways to increase the performance of data collection for such systems under the constraints of time delay, throughput, and finally, the working distance.

The thesis is organized into the following chapters. Chapter II introduces RFID technology and discusses the main components of a RFID system. It also describes the main principles of a RFID system concerning different types of communication between the reader and the tags. Finally, some important information from the digital communication theory that applies to RFID systems is given.

Chapter III presents the existing anticollision protocols used in RFID systems, and it evaluates the performance of each one and compares them in terms of throughput and time delay. Chapter IV, after a brief discussion of the most available standards, presents the proposed hybrid anticollision protocol in addition to the calculations for the maximum distance that can be achieved.

Finally, Chapter V discusses some applications of this technology and Chapter VI summarizes the conclusions of this research and proposes future work in this area.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND

A. INTRODUCTION

This chapter describes the main characteristics of Radio Frequency Identification (RFID) technology and the components of a RFID system. All the fundamental concepts of RFID technology, operation frequencies, and types of RFID components and advantages of this technology are also discussed in this chapter.

B. DESCRIPTION OF AN RFID SYSTEM

The RFID technology usually refers to the ability of the RFID system to detect and identify an object, which is in the interrogation zone of the system's reader with the use of radio frequency waves. The object carries a tag that communicates with the reader and transfers all the information. The transfer of data between the tag and reader is called *coupling.* Most systems use magnetic (inductive) or electromagnetic (backscatter) coupling [1] and [2]. RFID systems are robust and can perform under different environmental and operational conditions.

C. RFID ARCHITECTURE AND OPERATING PRINCIPLES

The mandatory components of a RFID system are the *tags* or transponders, the *reader* or interrogator together with the coupling devices (antennas) and the *controller*.

A *tag* is a device that carries the data of the object in which it is placed, and transmits those back to the reader using radio waves. A typical RFID system consists of one tag to hundreds of tags.

A reader or interrogator is the central unit of the RFID system. It can read, and in some applications, write the data from/to the tags. Some readers have built-in antennas.

A controller is needed to provide robustness to the system and is a mandatory component of new generation readers, which have this component built-in as well.

Furthermore, according to [3], optional components of the RFID system are the sensors, actuators and annunciators for providing external inputs and outputs to the

system, and finally, the host computers with the software, which controls reader behavior. All the above components, together with the communication infrastructure, collaborate and create the RFID network.

Figure 1 shows a typical RFID network. It consists of a reader with an external antenna, a tag and multiple sensors such as a photo eye and a motion detector, which transfer data to the reader (inputs) and an actuator/annunciantor as an output. Also, there are two computers with one to control the access of the reader to another network.

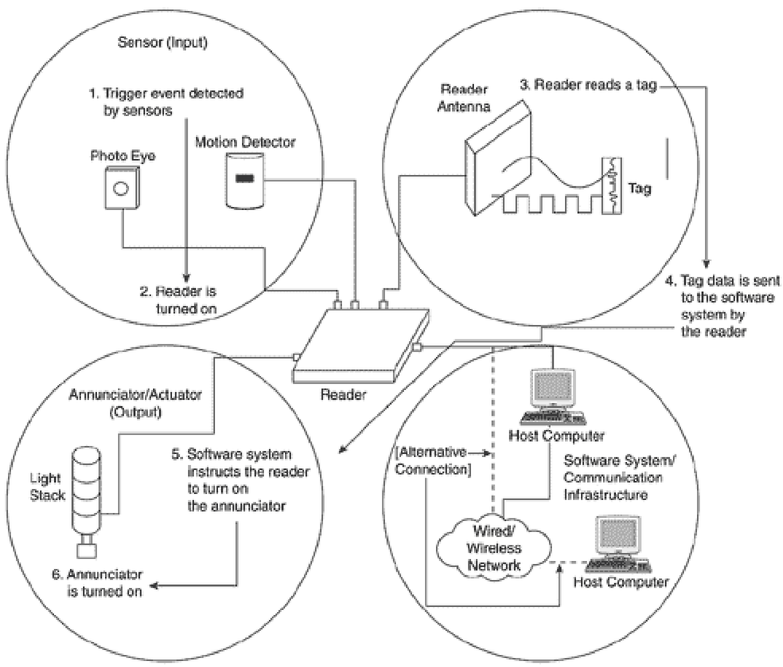


Figure 1. Typical RFID System (From Ref. 3)

The following paragraphs discuss, in more detail, the most important components of a RFID system: tags and readers.

1. Tags Properties and Classification

Radio frequency tags are devices that can only communicate with readers and are unable to communicate with each other.

There are three classifications of tags according to their attributes [3]. Tags are classified according to their design, type and memory.

Table 1 presents the most important characteristics of the tags according to their design (Intergraded circuit or Chipless tags), type of energy source (Passive, Active or Semi-active), and finally according to their memory (Read Only, Write Once/Read Many, and Read/Write).

Attributes	**Characteristics**
Design	• IC-Based − Has an intergraded circuit (microchip). • Chipless − Uses properties of tag's material to transmit the data. Can achieve better accuracy and highest range from IC-Based tags. It is powerless and without the ability to store new/additional data.
Type	• Passive − Powerless with lowest range (up to 3m), [2, 3] and accuracy. • Active − Requires battery to operate the microchip and to communicate with the reader. It has higher accuracy and can achieve a range of 15m and above [2]. • Semi-active− Battery supplies the power only to the microchip. Offers better range and accuracy than passive tags.
Memory	• Read Only − Data is written at tag from manufacture and cannot be changed. • Write Once/Read Many − Data is written once at any time. • Read/Write − Most flexible. Data can be overwritten.

Table 1. Tag Attributes and Characteristics (After Ref. 1].)

The most common tags are the passive tags with intergraded circuits with read-only memory because of their simplicity and lower cost than active and write memory tags.

Figure 2 shows the components of a passive tag; a microchip and a tag antenna. This is an IC-based tag, which is the most common in passive RFID systems. The size of RFID tags can be very small and depends mainly on the size of the antenna as shown in Figure 2 (chips can be extremely small).

The term Chipless tag refers to those tags that do not contain a microchip, but use materials properties to transmit the data. Although Chipless tags have greater reading

distance, lower cost, and better accuracy, they are only used for specific simple applications (i.e., handling RF interference [3]). This thesis investigates the RFID system using IC-based transporters. Passive tags use the transmitted power from the reader to transmit their stored data. The memory size of a tag depends on the application. It might be 1 bit (1-bit transponder) to more than 2 kbits for passive tags [3], or up to 64 Kbytes for active ones with write data capabilities (SRAM memory) [2].

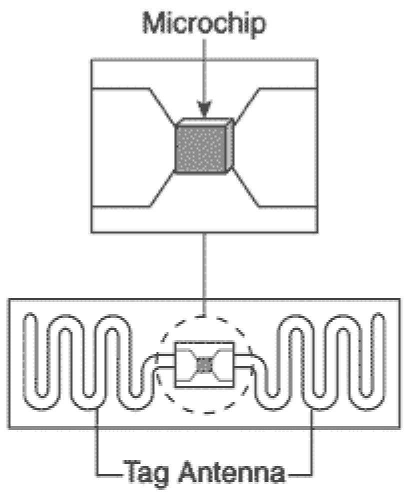


Figure 2. Passive Tag Components (From Ref. 3).

Figure 3 shows the basic elements of the microchip of Figure 2 for a passive tag. This microchip has a modulator for modulating the transmitted signal, a memory unit to store the identifying data, a power control/rectifier, which has a dual purpose: it protects the tag against overvoltage and also supplies it with DC power, and finally a clock and a logic unit.

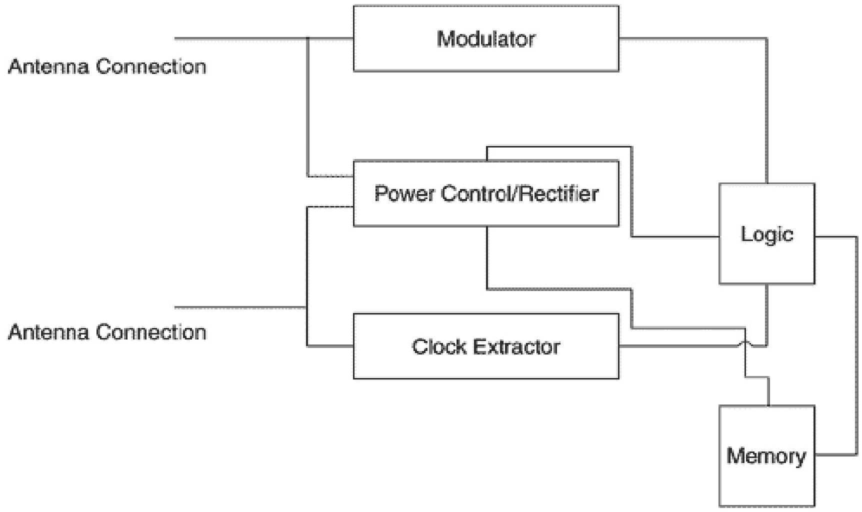


Figure 3. Elements of Microchip for Passive Tag (From Ref. 3)

The size of the antenna depends on the free space electromagnetic wavelength λ, which decreases when the operating frequency f increases, ($\lambda = \frac{c}{f}$). The higher the frequency, the smaller the antenna size. On the contrary, a smaller antenna means a shorter reading distance for a passive tag [4]. The purpose of the application will determine the choice. In this thesis, the operation frequencies will be in the microwave (ISM bands) and thus tags are assumed to be very small with no significant physical size.

The strength of the electromagnetic field of the reader is very significant for energizing the passive tags. This strength is a function of the distance r between the tag and reader, the operation frequency f and the gains of tag G_t and reader's antenna. G_r reduces as the free space path loss a_F given by the following equations increases:

$$\alpha_F = \frac{(4\pi)^2 r^2}{G_t G_r \lambda^2} \tag{2.1}$$

and in dB

$$a_F = -147.6 + 20\log(r) + 20\log(f) - 10\log(G_t) - 10\log(G_r)\,. \tag{2.2}$$

Equations 2.1 and 2.2 apply only in electromagnetic backscatter coupling RFID systems or long-range systems, which will be presented in detail in the next paragraphs. a_F is the free space path loss from the Friis equation which is inverse proportional ($P_{tag} \propto \frac{1}{a_F}$) to the power received at the tag antenna (P_{tag}).

Table 2 gives an idea of the free space path loss at different frequencies and distance between the tag and reader. The antenna of the reader is assumed to be isotropic (gain equal to one) and $G_T = 1.64(dipole)$. As seen for *Microwave* (2.45 GHz) frequencies, path loss increases significantly and thus reduces the reading distance.

Distance (r)	**Path loss at 868 MHz (UHF)**	**Path loss at 915 MHz (UHF)**	**Path loss at 2.45 GHz (Microwave)**
0.3 m	18.6 dB	19.0 dB	27.6 dB
1 m	29.0 dB	29.5 dB	38.0 dB
3 m	38.6 dB	39.0 dB	47.6 dB
10 m	49.0 dB	49.5 dB	58.0 dB

Table 2. Typical Path Loss Values (After Ref. 2.)

2. RFID Readers

RFID readers are the devices that control the exchange of data in a RFID system. All readers have an onboard controller, a transmitter and receiver antennas and communication functions if they are to communicate with a computer. Antennas might be built-in (in *handled* or *stationary* readers) or external devices (only in *stationary readers*). The controller is responsible for communication with the tags and controls the reader's behavior. The reader uses one or more antennas to communicate with the tags. An antenna transmits the reader's RF broadcast signal and receives the responses from the tags. Therefore, positioning the antennas around the tags may provide different accuracy in the collected data [3]. In other words, readers with external antennas can increase the reliability of the collected data by positioning optimal antennas near the tags using cables because:

- Signal-to-Noise Ratio increases due to the decrease of the distance r.
- Spatial Diversity.
- Multipath.

Figure 4 shows a typical stationary RFID reader in a UHF band with eight ports. Those kinds of readers provide more capabilities than the smaller ones and it is easier to carry handled readers.

Figure 4. Stationary RFID Reader (From Ref. 9)

Stationary readers like the one in Figure 4 operate either in autonomous or interactive mode.

a. Autonomous Mode (AS)

The reader continuously reads all the tags in the interrogating zone and saves every tag in the tag list. The tag can be stored in the tag list as long as the reader reads it or for a specific period of time after the last reading. This time period is generally called *persist time*. After that time, the reader deletes the specific tag from the tag list.

The tag list includes the following information [4]:

- Unique tag identifiers.
- Reader name.
- Reading time.
- The antenna ID that reads the specific tag.
- How many times the reader reads this tag.

b. Interactive Mode

In interactive mode, the reader executes commands from a host computer, which is connected to the RFID network. When the reader executes the last command, it sends a report to the *client* and waits for a new command.

3. Types of Coupling

Coupling is the mechanism by which energy transfers from the reader to the tags. There are three types of coupling systems [1, 2]:

- *Close coupling systems* (contactless smart cards), with a reading range up to 1 cm. Those systems use both electric and magnetic fields [1].
- *Remote coupled systems,* with reading/writing ranges up to 1 m. Those systems use an *inductive* (magnetic) coupling (also called *load modulation*) and a few of them use a *capacitive* (electric) coupling [1].
- *Long –range systems (LRS)*, with ranges of 3 m for passive and up to 15 m for active tags. Almost all LRS operate in UHF and microwave frequencies and use *backscatter modulation* for coupling [1].

This thesis is interested in RFID systems using backscatter modulation, which means tags are in the far-field of the reader.

Passive tags use a reader's energy to supply the microchip and then transmit the data to the reader, while active tags need it only for transmitting the data. Thus, the power salvaged from the tag is very important. Sufficient power strength in the antenna of the tag means that data can be transmitted. The power available in the tag, P_{tag}, is given by (2.3):

$$P_{tag} = \frac{\mathrm{P_r} G_r G_t \lambda^2}{(4\pi)^2 r^2} \tag{2.3}$$

where $\mathrm{P_r}$ is the transition power of the reader, G_r and G_t are reader's and tag's antennas gains, λ is the wavelength and d the distance between the reader and the tag.

4. Frequency Ranges of RFID Systems

The frequencies used in communication between the tag and the reader depend on the specific application. Many restrictions and regulations, such as maximum allowable power, exists in RFID systems [3]. Moreover, regulations are not the same worldwide.

Table 3 summarizes the most important available frequency ranges for different countries and Europe together with the effective radiated power (ERP). As seen from this table, only usable frequencies in the Lower Frequencies (LF) and Higher Frequencies (HF) bands are universally the same. Finally, it is important to mention that the transmitted power of 4 watts in the microwave band is at the reader's antenna.

Country /region	LF	HF	UHF	Microwave
U.S.A.	125-134 KHz	13.56 MHz (10 watts ERP)	• 888-889 MHz and • 902-928 MHz, (1 watt ERP or 4 watts ERP with directional antenna).	• 2.400-2.4835 GHz, (4 watts EIRP) • 5.725-5.875 GHz, (4 watts ERP)
Europe	125-134 KHz	13.56 MHz, (Power 42 dB μ A/m at 10m)	• 865-865.5 MHz, (0.1 watts ERP) • 865.6-867.6, (2 watts ERP) 867.6-868 MHz, (0.5 watts ERP)	• 2.400-2.4835 GHz, (10 mW EIRP) • 5.725-5.875 GHz, (25 mW EIRP)
Japan	125-134 KHz	13.56 MHz	Not Allowed	2.400-2.4835 GHz
China	125-134 KHz	13.56 MHz	Not Allowed	2.446-2.454 GHz, (0.5 watts ERP)

Table 3. International Frequency Ranges for RFID Systems (After Ref. 3)

Most of the applications in RFID systems are in *Industry, Scientific, and Medical* (ISM) bands (2.45 GHz and 13.56 MHz) and below 135 KHz (inductive coupling).

D. COMMUNICATIONS IN RFID SYSTEMS

The communication between the reader and the tags is similar to other digital communications systems. The data bits transmitted from the reader after *baseband coding* are also known as digital encoding format and *digital modulation*. Tags receive the data, demodulate them and then decode the data using signal coding. Communication between

the tags and the reader is exactly the same for all the tags. This type of communication is called full duplex. Both elements often have both a modulator and a demodulator (modem) [2].

Baseband coding is the representation of data in binary ones and zeros, while digital modulation is the transmission of the message signal in a higher frequency, which is called a carrier frequency by changing one of the signal parameters. The modulator modulates the binary sequences, which have been stored in the memory unit of the tag or the reader and transmits it as an analog waveform by using the right coding and modulation.

A description of baseband coding and digital modulation techniques used in RFID systems follows. Then, communication between the reader and the tags is discussed.

1. Baseband Coding

Baseband coding is necessary before transmitting the digital signal from the reader in an analog waveform. RFID systems use one of the following baseband coding procedures [2]: Non Return to Zero (NRZ), Manchester code, Miller code, Modified Miller code, Differential bi-phase (DBP), Unipolar RZ, differential coding, and Pulse-pause (PP) coding. The main characteristics of each one are discussed below [2, 5].

a. Nonreturn to Zero-Level (NRZ-L)

It is the easiest way to transmit digital signals. This code uses two different voltage levels for binary zero and binary one. Voltage has to be constant during a bit interval. Commonly, a binary one is represented by a higher level voltage (usually positive) and a binary zero by a lower level (usually negative).

b. Manchester Coding (Bi-Phase)

Manchester codes, also known as split-phase coding, have a transition at the middle of each bit period. In industry practice and in IEEE 802.3 standards, a transition from low-to-high (positive) represents a binary one and from high-to-low (negative) a binary zero [5]. This transition, except for the representation of the data, also provides a clocking mechanism for synchronizing the receiver. Finally, the transition in the Manchester code also provides error detection. Manchester coding is the most famous code for the forward link (reader to tags) and also very usable for the reverse link [2, 6].

c. Differential Biphase (DBP) Coding

In differential coding such as differential Manchester, the information signal is represented in terms of changes between the successive signal elements [5]. Besides the transition in the middle of each bit interval for binary zero and the lack of transition for binary one, there is also always a transition at the beginning of the bit duration (level inversion). The reason for this additional transition is the reconstruction of the pulse in the receiver.

d. Miller Coding

A transition in the middle of bit duration represents a binary one. In binary zero, the level of the next bit is the same as the level of the previous bit. Also, a sequence of zeros creates a transition in the beginning of the bit duration.

e. Modified Miller Coding

In this code, every transition is represented by a negative pulse with very short duration compared with the bit period. This type of coding is very often used in inductive coupling RFID systems because it can be assumed that the power supply from the reader to the tag continues even when data transfer takes place.

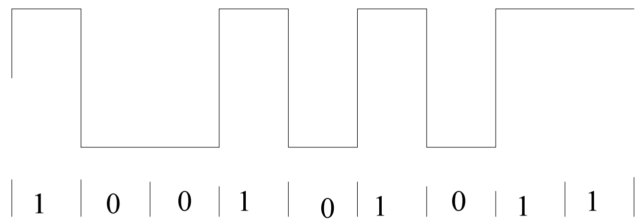
f. Unipolar Return to Zero (RZ) Coding

Binary zero is represented by a low level voltage for the entire bit period whereas a binary one is represented by a high level voltage in the first half of the bit period.

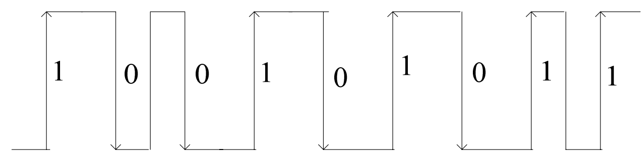
g. Pulse-Pause Coding

A binary one is represented by a pause of duration t before the next pulse and a binary zero by a pause of duration $2t$ before the next pulse. This coding is also used a lot in inductive coupling RFID systems like the modified Miller code. It is used for the data transmission from the reader to the tag for the same reason with the modified Miller code.

Figure 5 shows the NRZ and Manchester coding for the data stream100101011. It shows the transition at the middle of each bit period for the Manchester coding, a property very important in RFID systems.



a.



b.

Figure 5. Baseband Coding in RFID Systems: (a.) NRZ and (b.) Manchester Codes.

2. Digital Modulation

Digital modulation or band-pass modulation is the process in which one or more of the characteristics/parameters of the carrier signal (electromagnetic wave) is/are changed. Modulation is used in the transmitter and the detection/demodulation of the signal is used in the receiver. In RFID systems, both end-to-end components have a circuit for each of the above processes.

The parameters of the carrier that can be changed are: amplitude (power), phase and frequency. The digital modulation used in RFID systems are the binary amplitude shift keying (ASK), binary frequency shift keying (FSK) and binary phase shift keying (PSK). A brief discussion of each is given in the following paragraphs.

a. Amplitude Shift Keying (ASK)

In binary ASK modulation, a sinusoidal carrier is used and its amplitude varied between a fixed value A_c (in a fixed frequency f_c) for a bit duration T_b, which represents a binary one and a value equal to 0 for a bit duration T_b, which represents a binary zero.

It is easy to generate ASK by applying the incoming data (baseband signal) to the sinusoidal carrier in a product modulator. Moreover, it is possible to detect

it with a very simple demodulating circuit. For this reason, it is primarily used in communication from the reader to the tag. If $s(t)$ is the binary ASK signal, it can be represented as follows [7]:

$$s(t)=\begin{cases} A_c\cos\left(2\pi f_c t\right), & symbol\,1 \\ 0, & symbol\,0 \end{cases}. \tag{2.4}$$

b. Phase Shift Keying (PSK)

In binary PSK, the phase of a sinusoidal carrier is changed. Both symbols have the same amplitude A_c and frequency f_c but a different phase of 180° separation. A binary PSK signal $s(t)$ can be expressed as [7]:

$$s(t)=\begin{cases} A_c\cos\left(2\pi f_c t\right), & symbol\,1 \\ A_{cc}\,\mathrm{os}\left(2\pi f_c t+\pi\right), & symbol\,0 \end{cases}. \tag{2.5}$$

c. Frequency Shift Keying (FSK)

In binary FSK, the frequency f_c of the carrier is changed. Each symbol is represented by a sinusoidal wave with the same amplitude and phase but different frequencies, f_1 *and* f_2. A binary FSK signal s(t) can be expressed as [7]:

$$s(t)=\begin{cases} A_c\cos\left(2\pi f_1 t\right), & symbol\,1 \\ A_c\cos\left(2\pi f_2 t\right), & symbol\,0 \end{cases}. \tag{2.6}$$

Figure 6 gives an example of digital modulation for the data stream 0101100100100 . Note how the phase changes 180° in (d) each time the data bit changes.

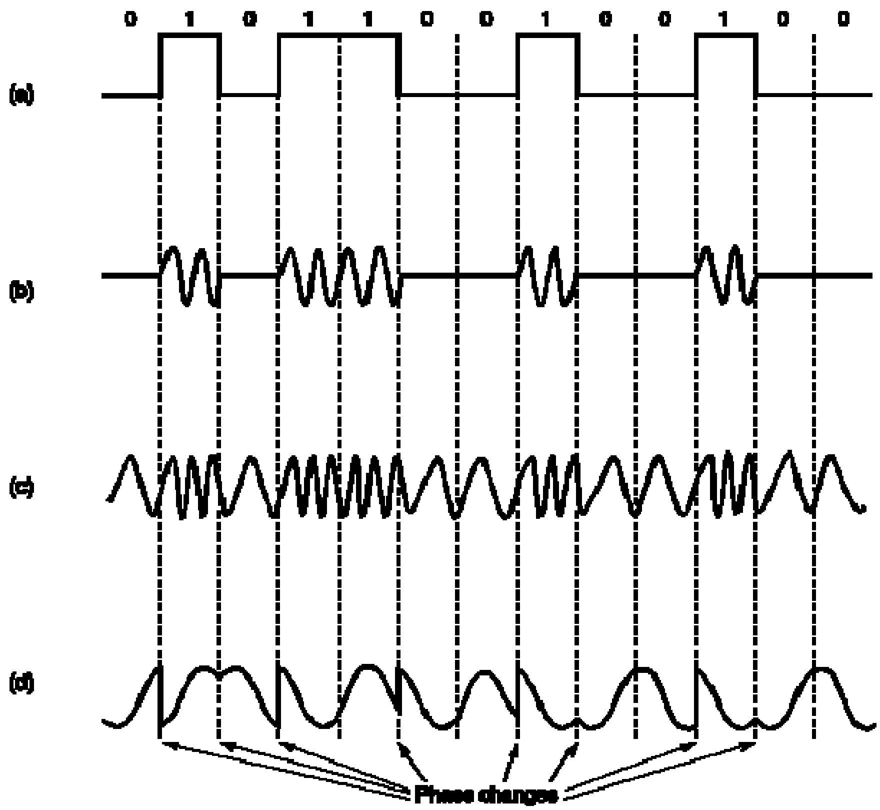


Figure 6. Binary Digital Modulation. (a) Baseband Signal (b) Amplitude Shift Keying. (c) Frequency Shift Keying. (d) Phase Shift Keying. (From Ref. 8)

3. Communication between the Reader-Tag and Tag-Reader

There are two types of communication in RFID systems. The first type is one-to-one communication between the reader and the tag, such as in contactless smart cards and in electronic pay collection systems (EZ pass). In this kind of system, only one tag is in the interrogation zone of the reader and communication is simple. On the other hand, data transfer is more complicated in systems with more than one tag in the interrogation zone of the reader. More sophisticated software and hardware are needed for those systems.

This thesis studies the data transfer in the second type of RFID systems. The communication procedure in those systems is as follows [10]:

- The reader transmits broadcast signals to all tags. Selective communication can only be achieved at the upper protocol layer.
- All tags in the interrogation zone of the reader receive the signal, energized, supplies the IC and replies to the reader's signal through the same channel. Hence, multiple signals are received in the reader's antenna and collision might occur.

- The reader waits for a predetermined period of time before retransmission.
- Tags reply or stay silent according to the reader command.
- After the time period has passed, the reader receives all the responses from the tags and proceeds to the next command.

4. Electronic Product Code (EPC)

EPC is a numbering format, which was developed by the auto-ID center at the Massachusetts Institute of Technology (M.I.T.). The purpose of EPC is to provide a unique identifier to any physical object in the supply chain [1]. EPC will replace the Universal Product Code (UPC), which is in use today and supports barcodes. The EPC global network is a non-profit organization which promotes EPC to become a worldwide standard for accurate and automatic identification of all items in the supply chain [11].

The format of the EPC type I consists of 96 bits length (there is also a type with 64 bits) and consists of the following four fields [1, 10]:

- Header, which identifies the EPC's version number, length, type, structure, and generation of EPC. The header is 8 bits in length.
- Manager number, which identifies the enterprise using the EPC number.
- Object class, which refers to the class or category of the product.
- Serial number, which identifies a specific instance of the tagged item. The serial number is 38 bits in length.

Figure 7 presents an example of the EPC numbering format. This product has a header of 233 and it identifies the enterprise with manager number 7809R6. The serial number 001238T9 might identify chocolate milk with a specific product date.

The header and manager fields are assigned from the EPC global network while the object Class and serial number by the specific enterprise (company).

2 3 3.	7 8 0 9 R 6 .	3 4 5 6 7 6 .	0 0 1 2 3 8 T 9
Header	Manager number	Object class	Serial number

Figure 7. EPC Numbering Format

5. The Open System Interconnection Model (OSI)

In order to discuss the protocols used in RFID systems in subsequent chapters, it is important to introduce the open system interconnection reference model (OSI). The OSI was developed by the international organization for standardization (ISO) as a technique of layering the communication functions between two or more devices. The OSI model has seven layers. Each layer performs a specific function, which allows this system to communicate with another system and provides services to the next higher layer [5].

Table 4 illustrates the seven layers of the OSI model with a brief definition. Some of the main principles in defining the OSI model are [5]:

- Try to keep the number of layers as low as possible.
- Similar functions will be collected in the same layer.
- Layers must have flexibility in future changes.
- Any kind of change in functions or protocols in one layer should not affect other layers.
- Layers should be created when needed to handle the data in a different way.
- Two or more sublayers might be in the same layer to provide interface with adjacent layers.
- Allow bypassing of sublayers.

Application (Layer 7) Provides access to OSI environment for users and distributed information services.
Presentation (Layer 6) Provides independence to the application processes from differences in data representation (syntax).
Session (Layer 5) Provides the control structure for communication between applications. Establishes, manages and terminates connections between applications.
Transport (Layer 4) Provides reliable and transparent transfer of data between end systems, or hosts. Also provides end-to-end error recovery and flow control.

Network (Layer 3) Provides upper layers with independence from data transmission. Provides routing and switching technologies and creates logical paths for transmitting data from one node to another. It is responsible for addressing, error handling, congestion control packet sequencing and for establishing, maintaining and terminating connections.
Data Link (Layer 2) Provides reliable transfer of data across the physical link. Here data packets are encoded and decoded into bits. It sends frames with necessary synchronization, error control and flow control. It is divided into Media Access Control (MAC) and Logical Link Control (LLC) sublayers.
Physical (Layer 1) It is responsible for transmitting the bit stream over the physical medium. It provides the necessary hardware for sending and receiving data on the network. It deals with the mechanical, electrical, functional and procedural characteristics to access the physical medium.

Table 4. The OSI Layers (From Ref. 5.)

In general, each layer has its own protocol, which allows it to communicate with the same layer of another system or node. The connections for all the layers are logical except for the last one, which is the physical layer. The data exchange between two layers always occurs from the connection at the physical layer. All data are transferred from the higher to lower layers in packets.

Chapter III explains the protocols (anti-collision algorithms) proposed for RFID systems in order to simulate their performance and efficiency in data transfer from the tags to the reader.

THIS PAGE INTENTIONALLY LEFT BLANK

III. DATA INTEGRITY AND ANTI-COLLISIONS PROTOCOLS

A. ANTI-COLLISIONS PROTOCOLS

This thesis focuses on passive Radio Frequency Identification (RFID) systems using backscattering modulation in microwave (2.4 GHz) and ultra high frequency (UHF) bands, where the transmission rate is very high. Therefore, the following discussion refers to those RFID systems.

The main disadvantage in RFID communications is the multi-access that occurs in uplink, where multiple tags respond to the reader's signal-command. Multiple responses at the same time on the Radio Frequency (RF) communication channel means that the reader cannot identify the data transmitted from the tag. This event is called tag *collision* and is responsible for the low tag identification efficiency [2] in RFID systems.

Data integrity in RFID systems also depends on the following parameters:

- Power received from the tag. This power should be efficient to energize the circuit of the tag and also transmit the data to the channel.
- Signal-to -Noise Ratio (*SNR*) in the reader. The received signal in the reader should be high enough so the reader will be able to verify the data sequence. Some kinds of Error Detection (usually Cyclic Redundancy Check) need to be used in the reader.

In the following discussion, it is assumed that the above parameters are satisfied in the development of an efficient anticollision algorithm.

Space Division Multiple Access (SDMA) and Frequency Division Multiple Access (FDMA) are not generally used in RFID systems because of the high cost to implement them. Both of the above anti-collision techniques are limited to "a few specialized applications" according to [2], and therefore, are not suitable for passive RFID systems, which need to have a low implementation cost and complexity.

Time Division Multiple Access (TDMA) is an excellent choice for RFID systems with a small number of tags. If the number of tags is large and not known during the process of identification, the *Packet Radio* (PR) technique is by far the best anti-collision

technique used in RFID systems. The advantage of PR technique is that it allows the reader to identify a large number of tags with a small amount of overhead. Also, it is not a requirement for the reader to know the number of tags in the RFID system.

Two main procedures of PR are used according to [2]. In the asynchronous procedures, the reader does not control the tags inside the interrogation zone. Asynchronous procedures are also called *transponder-drive*; the most important of this kind of PR is the PURE ALOHA procedure which is used in passive RFID systems for its simplicity. On the other hand, in the synchronous procedures, which are *reader-driven*, the reader identifies all the tags inside the interrogator area by a unique serial number assigned to each tag. *Reader-driven* procedures are divided into *polling* and *binary search* procedures. Most of the standards for the UHF RFID systems propose Aloha-based anti-collision algorithms that are probabilistic and binary tree search anti-collision algorithms that are deterministic [11].

In passive RFID systems, tags are powerless and stateless devices that cannot sense the channel. They do not know about the existence of other tags in the neighboring area and cannot detect when a collision occurs. Thus, the reader is responsible for implementing an anti-collision algorithm and controlling collisions. This algorithm must be simple without numerous computations in the transponders. In order to increase the low efficiency of the PURE ALOHA algorithm, a variation of it is used which is called *Slotted Aloha.*

In a Slotted Aloha algorithm, the reader controls and synchronizes the tags before they respond.

This chapter focuses on the description of those algorithms and an evaluation of their performance in terms of *throughput* efficiency and *time delay*, which is the time needed by the reader to read all the tags in the area.

B. ALOHA-BASED ALGORITHMS

1. Basic ALOHA Procedures

The Aloha procedure or algorithm is a probabilistic procedure, which can be used in the multi-access uplink communication from the tag to the reader to avoid collision. It is very simple to implement, and thus currently, it is very common in passive RFID systems with read-only tags.

In RFID systems using Aloha anti-collision algorithms, the time each tag uses for the transmission of data is a small fraction of the repetition time and long pauses between transmissions from the same tag occurs. Thus, the communication between the reader and the tags is not continuous. In addition, each tag occupies in general a different period of time to transmit the data [2], which depends on the amount of data to be transmitted.

As a result of the simplicity of the Aloha algorithm, there is a high possibility of collision between tags because tags can transmit their data to the reader randomly at any time. This possibility increases while the offered load G is increased. The average utilization or throughput S of the channel is given by equation (3.1).

$$S = G \cdot e^{(-2G)} . \tag{3.1}$$

The Aloha algorithm has a maximum of 18.4% utilization at $G = 0.5$, and for this reason, the Aloha algorithm has been modified to improve efficiency up to 36.8%. This modification is called Slotted Aloha. The average utilization in Slotted Aloha is given by equation (3.2) and has a maximum value of $G = 1$.

$$S = G \cdot e^{(-G)} \tag{3.2}$$

In Slotted Aloha, the time of the channel is divided into uniform slots with size equal to the transmission time. Currently, tags transmit the data packets only at the beginning of each slot [2, 3]. Consequently, synchronization is necessary in the Slotted Aloha algorithm. The necessary synchronization is provided by the reader, and therefore, Slotted Aloha is a reader-driven TDMA procedure [2].

Figure 8 illustrates the performance of the Slotted Aloha algorithm. It can be seen that while the offering load (G) increases, throughput (S) increases until the maximum

value of 36.8%, and then falls rapidly for values of the offering load greater than 1. This is a main disadvantage of the Slotted Aloha algorithm because the system is unstable, and with low efficiency.

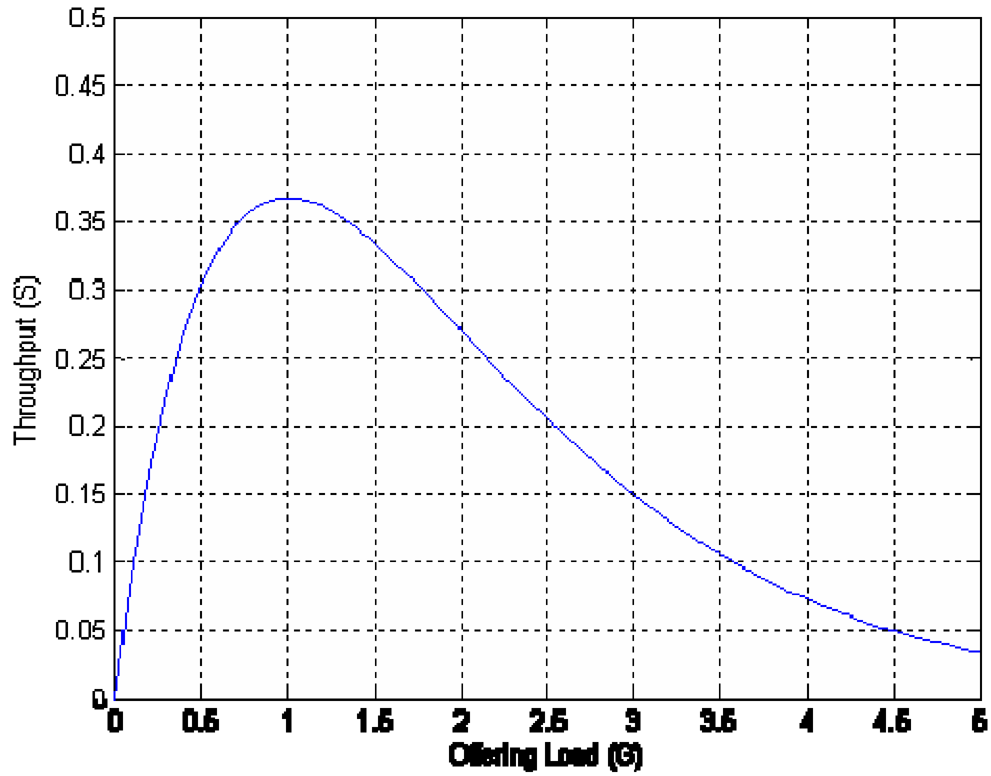


Figure 8. Efficiency in Slotted Aloha

A variation of Slotted Aloha is used in RFID systems and has been proposed by the International Organization for Standardization (ISO) and the Electronic Product Code (EPC). This variation of Slotted Aloha in RFID systems is called *Framed Slotted Aloha* (FSA). In the following subsection, the FSA and dynamic FSA are reviewed and examined.

2. Framed Slotted Aloha (FSA) Algorithm

The Framed Slotted ALOHA (FSA) algorithm is a Slotted Aloha in which the available timeslots where the tags can respond to the reader commands are organized into time frames. Each frame is divided into a number of slots (usually powers of 2) and each

timeslot is long enough for the tags to transmit their data. Those time frames have duration equal to the time between two REQUEST commands of the reader [2, 11]. Thus, the efficiency of the FSA remains the same as in Slotted Aloha.

In order to discuss the FSA algorithm, it is necessary to present the commands that a reader transmits to the tags [2]:

- REQUEST: This is the first command transmitted by the reader in order to synchronize the tags into the interrogation zone, and also energizes the tags with the RF energy so tags can randomly select one slot in the frame and transmit their data (Serial Numbers).
- SELECT: Prompts only the tag with the same Serial Number (SN) with the one that has been transmitted from the reader to respond.
- READ_DATA: Reader reads the selected tag.

If the frame size is fixed during the procedure of identification, FSA is known as Basic Framed Slotted Aloha (BFSA). An example of how the BFSA algorithm works is given in Figure 9.

In the example, it is assumed that the length of the SN is 16, so it can support a maximum of $2^{16} = 65536$ tags. Let n be the number of tags that is actually inside the interrogation zone of the reader when the first REQUEST command is sent. If the RFID system has $N \leq 65536$ tags and $n \leq N$, then each tag randomly selects one of the k available slots and transmits the SN which has been assigned to this specific tag. In the first time slot tags, 2 *and* 3 did collide (select the same slot), while tags 1 *and* n did not collide (only one tag in slots two and k) and they have been identified by the reader. The reader then selects the tags that did not collide and reads them. It also stores the selected tags in its memory and then transmits another REQUEST command to identify more tags. This procedure continues until all the tags in the interrogation zone have been read.

If the number of tags into the interrogation zone increases, collisions between tags is increased because more tags randomly select the same time slot. Thus, the efficiency in the RFID system decreases and FSA needs to be modified in order for the RFID system to operate in the area of maximum efficiency. The throughput versus offering load for

FSA is also given by Figure 8. Therefore, maximum efficiency occurs when the offered load G is equal to 1, i.e., the number of slots are equal to the number of tags in the interrogation zone.

Downlink	REQUEST	Slot # 1	Slot # 2	Slot # 3	…	Slot # k	REQUEST
Uplink		Collision	Identification			Identification	
Tag 1			1110111011101110				
Tag 2		1111011110111110					
Tag 3		1111111111111111					
…….							
Tag n						0000000000000000	

Figure 9. BFSA Procedure in RFID System (After Ref. 2)

A modification of FSA is the *Dynamic Framed Slotted Aloha* (DFSA), which dynamically changes the frame size to increase tag identification, and thus, increases the efficiency in collecting the data from the tags.

3. Dynamic Framed Slotted Aloha (DFSA)

The *Dynamic Framed Slotted Aloha* (DFSA) algorithm was first introduced in [12] for multiuser channel-environments and proven to increase the upper bound of the FSA algorithm to 42.6%, and also increased the stability of the multiuser channel (system works in the area of maximum efficiency of Figure 8, which means that the offered load is almost 1); of course in [12], the author takes into account the capture effect. In [13, 14], DFSA was introduced for passive RFID systems where the number of tags is unknown.

If in FSA the frame size is too big to avoid collisions, and the number of tags in the area is too small, the performance of the system is reduced [2, 11], because the system performs in the left area of Figure 8, for G much less than 1. In specific

applications where the number of tags is known, it is constant through time, and if it is not too big, FSA can be used; otherwise, *Dynamic Framed Slotted Aloha* is the solution.

In DFSA, the reader has the flexibility to vary the frame size. Hence, it varies the number of available slots for the tags. If the reader does not detect tags, which means that collisions occur, it increases the frame size until an efficient number of tags can be detected. As long as tags are detected, it decreases the frame size and so on [11, 15].

The reader tries to identify all the tags in the interrogation zone in multiple *read cycles*. The amount of time in one read cycle is equal to the time elapsed between two REQUEST commands sent by the reader. The subject of this research is to investigate how the reader can detect and read the maximum number of tags with a minimum number of *read cycles* and a maximum probability of detection.

Much research has been done about the criterion which must be used in order to change the frame size. In passive RFID systems, the reader waits for the tags to respond and changes the frame size after each *read cycle* according to the number of tags in the interrogation zone. Thus, the criterion in DFSA is that the reader needs to estimate the number of tags in the previous read cycle and then adjusts the frame size accordingly. In section C, the system efficiency of DFSA and FSA is studied.

C. SYSTEM EFFICIENCY IN RFID SYSTEMS WITH DFSA AND FSA ALGORITHMS

In order to measure the efficiency of DFSA in a passive RFID system, the following assumptions must be made to decrease the complexity of the problem in the next paragraphs:

- Tags that have been read once from the reader in a previous read cycle, after activation, will not send their data again (Identification Number) if they re-enter the reader's field. This is like using the "*kill"* command from the reader. If this assumption is not valid, as it is for tags that need to be read more than once, the efficiency of the DFSA algorithm is less than the following calculations. It will be assumed that tags after reading will not respond to future reader requests [11].
- In the estimation of the number of tags in the reader's field, the *Capture Effect,* is assumed to be negligible. This effect helps tags near the reader to transmit their data although collision had occurred in the time slot they used. This happens because their signal is stronger than the farthest tags

due to channel attenuation. Capture effect increases the throughput of the DFSA algorithm and thus increases the overall efficiency of the RFID system [2].

- The communication channel, both uplink and downlink, is assumed to be noise free. Increasing noise decreases the ability of the reader to read the data from the tags, and thus decreases the performance of the system.

In DFSA, the reader estimates the total number of tags in the interrogation zone by using the received information from the slots in each frame as a feedback control. Thus, a controller is necessary. This is not a problem because as mentioned in the previous chapter, all modern readers have an onboard controller.

1. Estimation of Frame Size and Number of Tags in RFID Area Using the DFSA Algorithm

In the description of the DFSA algorithm that follows, the approach and methodology of [11, 15] is used.

Let N be the random variable representing the number of slots that have been used from the reader at the previous read cycle. Also, let E, R and C be the random variables representing the number of slots of the frame, which are empty, selected by only one tag, and finally selected by more than one tag, respectively. Finally, n denotes the number of tags in the interrogation zone, which is also a random variable.

Slots that have been selected by only one tag are the slots that the reader can read the data from the tag and identify it. In slots that have been selected by more than one tag, collision has occurred and the reader cannot identify the tags.

The probability p of a tag selecting a specific slot is given by:

$$p = \frac{1}{N} \tag{3.3}$$

and the probability for a tag to transmit its data (P_{read}) in this slot is given by:

$$\mathrm{P}_{read} = \left(\frac{1}{N}\right) * \left(1 - \frac{1}{N}\right)^{n-1} \tag{3.4}$$

because the selection of the slot from the tags is random, and every tag selects a slot independent of the rest $n-1$ tags with the same probability.

When the reader uses a frame size of N slots, the probability that k out of n tags to select a specific slot and not the others is binomially distributed [12] and is given by:

$$\mathrm{P}[R=k]=\binom{n}{k}*\left(\frac{1}{N}\right)*\left(1-\frac{1}{N}\right)^{n-1}. \tag{3.5}$$

While the probability that k tags transmit their data in the same slot [11, 15], (each slot is occupied by k tags out of n) is given by equation 3.6:

$$\mathrm{P}[C=k]=\binom{n}{k}*\left(\frac{1}{N}\right)^{k}*\left(1-\frac{1}{N}\right)^{n-k}. \tag{3.6}$$

The number k of the tags that occupy a specific frame slot is known as the *occupancy number* of the slots [11]. The expectation of the number of slots with k tags for the binomial distribution is given by equation 3.7:

$$\begin{aligned} &E\left[C=k\right]=N*\mathrm{P}[C=k]=N*\binom{n}{k}*\left(\frac{1}{N}\right)^{k}*\left(1-\frac{1}{N}\right)^{n-k} \\ &\Rightarrow E\left[C=k\right]=\binom{n}{k}*\left(\frac{1}{N}\right)^{k-1}*\left(1-\frac{1}{N}\right)^{n-k} \end{aligned}. \tag{3.7}$$

The time delay T which is necessary for each tag to transmit its Identification (ID) successfully is:

$$T=N*i \tag{3.8}$$

where i is the number of read cycles or number of retransmissions.

Let P_{empty} be the probability a slot is empty, and P_c is the probability that a collision has occurred in a slot. Then:

$$P_{empty}=\left(1-\frac{1}{N}\right)^{n} \tag{3.9}$$

and

$$P_c=1-P_{empty}-P_{read}. \tag{3.10}$$

The optimal frame size $N_{optimal}$ for the next read cycle can be calculated two ways [11], as given below:

- Maximizing the throughput S of the RFID system, which is defined as:

$$S = \frac{\Pr obability\ of\ reading\ a\ tag}{P_{total}} = \frac{P_{read}}{P_c + P_{read} + P_{empty}}$$
$$= \frac{P_{read}}{(1 - P_{read} - P_{empty}) + P_{read} + P_{empty}} = P_{read} \qquad . \qquad (3.11)$$
$$\Rightarrow S = \frac{1}{N} * (1 - \frac{1}{N})^{n-1}$$

- Minimizing the time delay T which is given in [11] as:

$$T = \frac{N}{(1 - \frac{1}{N})^{n-1}} . \qquad (3.12)$$

Figure 10 shows the behavior of the RFID system if the FSA algorithm and equation 3.10 are used. It is obvious that when the number of tags in FSA is far enough away from the selected frame size, then the system's efficiency decreases and the RFID system is unstable.

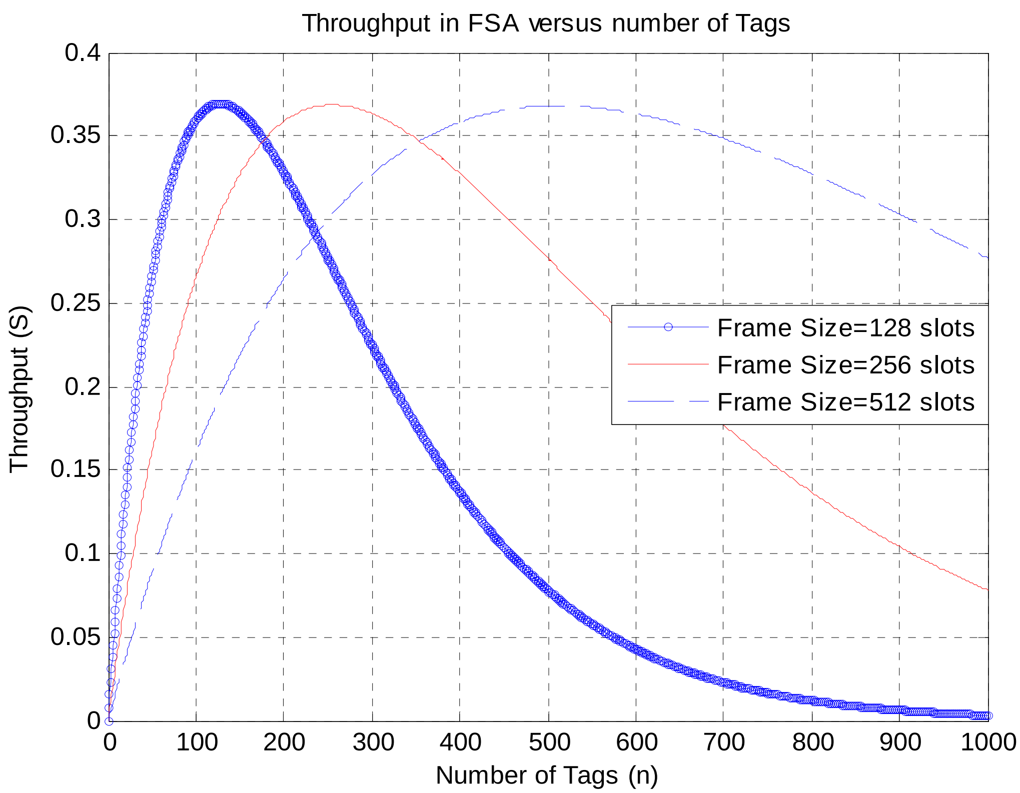


Figure 10. Throughput S in FSA for Different Frame Sizes

Both the above methods provide the same solution [11] for the $N_{optimal}$, which is $N_{optimal} = n$. Therefore, $p = \frac{1}{n}$. Thus, in DFSA, if the reader allocates a frame size equal to the number of tags in the interrogation area, the efficiency of the RFID system increases. The only problem now is that the reader needs to estimate this number of tags n in the area before it transmits the next REQUEST command.

Figure 11 illustrates the stability in throughput efficiency provided that the DFSA algorithm is used, and so $N_{optimal} = n$ is selected in equation 3.10 from the reader in every next duty cycle. The figure shows that throughput S is always equal to the maximum theoretical value of 36.8% of the Slotted Aloha protocol regardless of n. Moreover, there is a spike at the beginning of both subplots because when there is only one tag in the area,

the probability for a tag to collide in practice is equal to one and the reader always read this tag and so $S = 1$. After some tags are added, throughput falls very quickly to its final value.

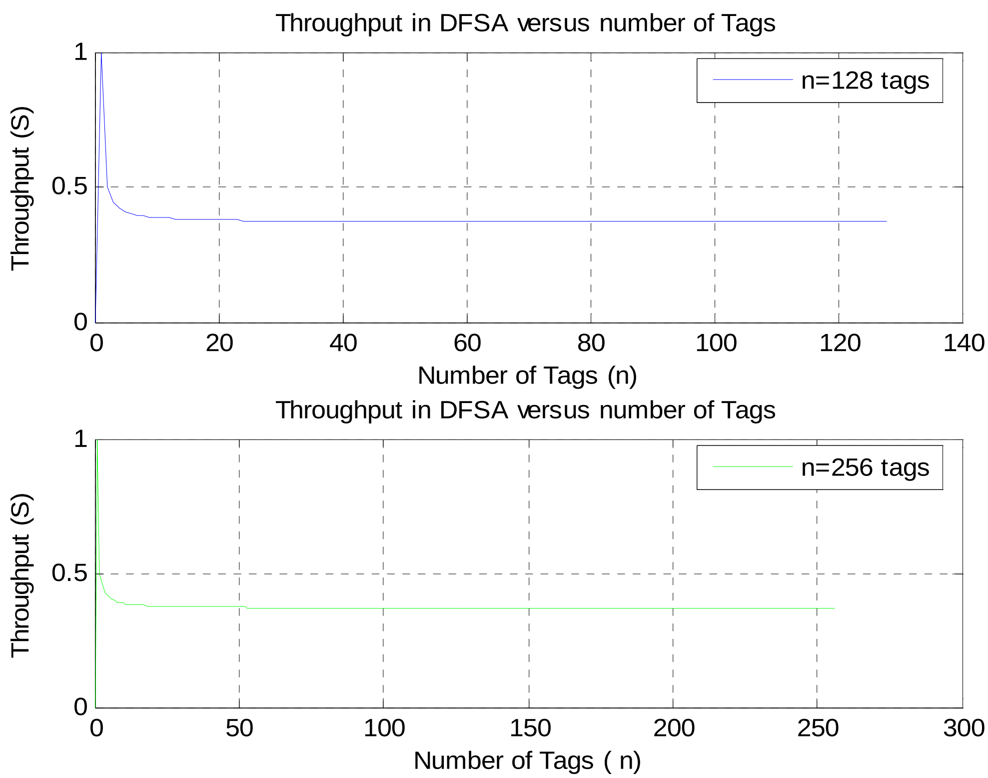


Figure 11. Throughput S in DFSA with Optimal Frame Size Selection

Figures 12 and 13 illustrate the time delay time (T) in both FSA for different frame sizes, and DFSA for $n = 0$ *to* 512 *tags*. In DFSA, it is assumed that the reader's initial frame size is equal to the optimal, which in practice is not always true. Figure 12 show that the DFSA algorithm increases the performance of the RFID system in terms of the time delay. T is greater if the FSA algorithm is used. The performance of the FSA algorithm decreases as the difference between n and N increases.

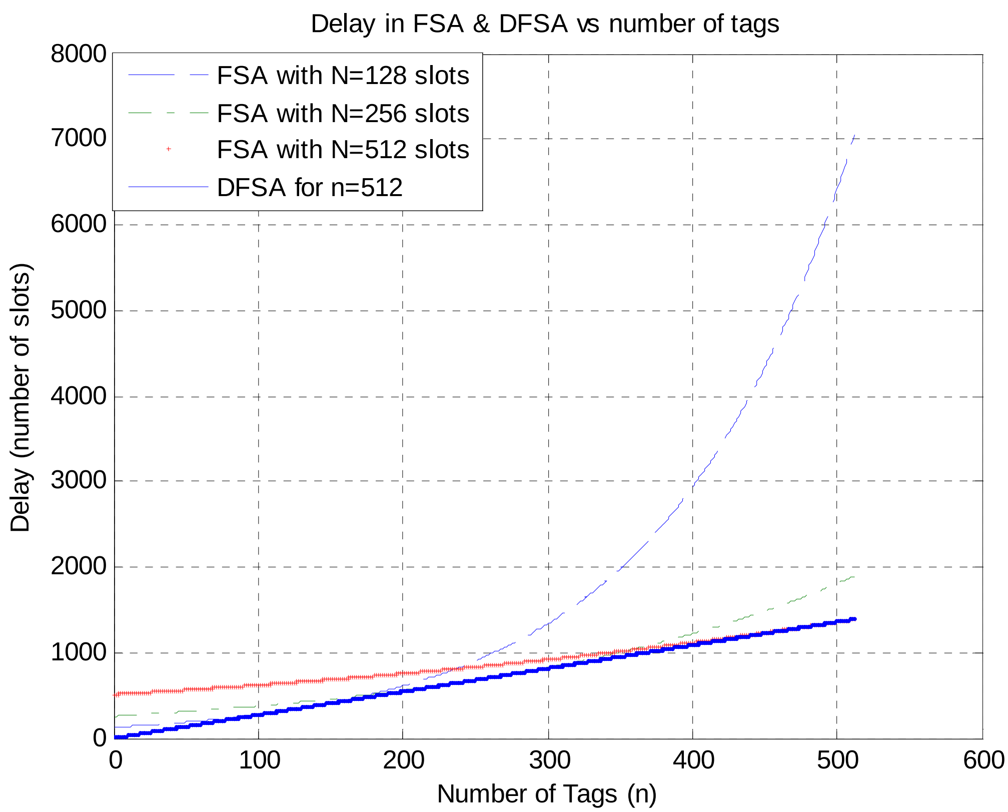


Figure 12. Performance of RFID System in Terms of Time Delay

Figure 13, which is just a magnification of Figure 12 in the area around 280 tags, shows that although FSA with $N = 512$ and DFSA seem to have the same behavior; this is only true when the number of tags is near 512 (actually for $n \geq 350$ *tags*). For a small number of tags ($n \leq 220$ tags), FSA with $N = 512$ gives the worst performance.

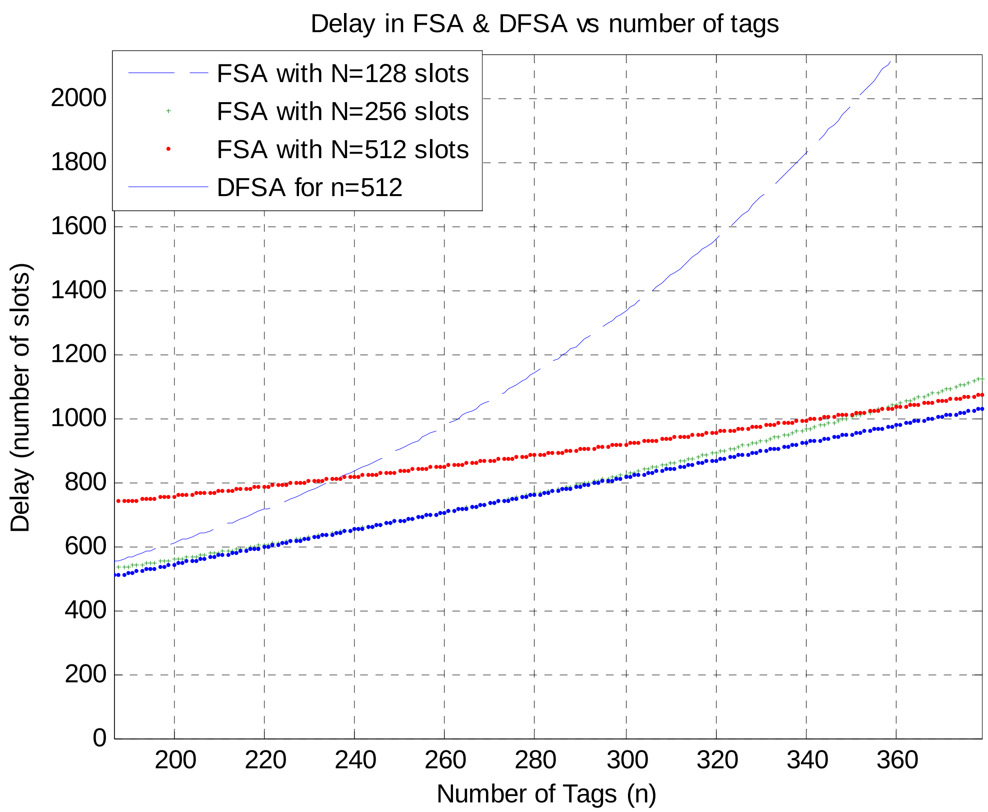


Figure 13. Magnification of Figure 12 in the Area for n=280

2. Developments in DFSA Algorithm

In [16], the authors proposed an alternative probabilistic Aloha-type anticollision protocol for RFID systems. It is called *Enhanced Dynamic Framed Slotted ALOHA* (EDFSA), which is similar to the DFSA algorithm with one difference. After the estimation of the number of tags in the area reader:

- if the number of tags n is $n \geq 177$, it divides the tags into smaller groups (called 'Modulo operation'), and thus, a smaller frame size is used (always $N = 256\ slots$) as seen in Table 5 or,
- if the number of tags is smaller than 177, then the DFSA algorithm is used.

Table 5 summarizes the EDFSA algorithm showing how the module works to keep the frame size constant at 256 slots.

The number of unread tags	Frame Size	Modulo (M)
⋮	⋮	⋮
1417 – 2831	256	8
708 – 1416	256	4
355 – 707	256	2
177 – 354	256	1
82 – 176	128	1
41 – 81	64	1
20 – 40	32	1
12–19	16	1
6–11	8	1
⋮	⋮	⋮

Table 5. EDFSA Algorithm (From Ref. 16)

Although the author's simulations in [16] showed improvement in system efficiency versus frame size, this method needs extended calculations in the reader and increases the tag's complexity and power consumption, something which is critical in passive RFID systems, because tags are powerless. For this reason, the next chapter proposes a new type of DFSA anticollision protocol based on simplicity and the constraint of minimizing power consumption in the transponder (tag).

Moreover, in both DFSA and EDFSA algorithms, the authors, although they mention which estimation function they use for estimating the number of tags n in the area, they do not provide any information on how this is done.

The reader can only calculate the number of tags that responds without collision which is represented by the random variable R given above. Also, the reader can calculate the number of slots with collision (given by random variable C) but how it estimates the number of tags that collides is unknown.

It is known that for every slot that collision occurs at least two tags have transmitted their data to it. Thus, a lower bound for the number of tags in the interrogation zone n, and therefore, the number of slots N that the reader must use in the next frame, is given by [14]:

$$N = R + 2C \,. \tag{3.13}$$

THIS PAGE INTENTIONALLY LEFT BLANK

IV. A PROGRESSING SCANNING (PS) TECHNIQUE FOR INCREASING THE PERFORMANCE OF RFID SYSTEM

A. STANDARDS FOR MICROWAVE PASSIVE RFID SYSTEMS

This chapter presents an alternative *Hybrid* anticollision protocol based on the Framed Slotted Aloha (FSA) algorithm for microwave RFID communication systems at 2.45 GHz. The parameters of the communication system will be according to those established in [17] by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) for *MODE 1* systems, which are the passive backscatter RFID systems of interest.

The parameters to take into consideration for the protocol to be proposed later are those concerning the physical link and the Media Access Control (MAC).

The most important of those parameters are the following [17]:

- The maximum transmitted power ($P_{r,\max}$) measured at the reader's antenna is 4 Watts (36 dBm) EIRP.
- The modulation, which is used in the forward link (reader to tag), is Amplitude Shift Keying (ASK as this is the simplest waveform, and can be detected easily by the tag with a simple circuit).
- The modulation, which is used in the reverse link (tag to reader), is Backscatter Modulation (BM).
- The data coding is Manchester for the forward link and FM0 (Bi-Phase Space) for the reverse link. FM0 is actually a differential Manchester technique as described in Chapter II.
- Both the tag and the reader have error detection capability by using a cyclic redundancy check (CRC) with 16 bits.
- The data bit rate should be between 30 to $40\,Kbps$ in both directions.
- Tags use the reader's signal for synchronization.
- The maximum occupied channel Bandwidth (BW) is 500 KHz.
- The memory size of the tags varies from 8 bytes to 64 bytes.

Moreover, it will be assumed that the chips of the tags are using the current semiconductor technology which decreases the power consumption in the tag, and a minimum power received ($P_{tag,\min}$) equal to $50\ \mu watts$ is enough in the antenna of the tag [2] for the tag to be capable of transmitting the data stored in its memory.

B. THE PROPOSED PROGRESSING SCANNING ALGORITHM

1. Maximum Distance of the RFID System

First, it is important to evaluate the maximum distance ($r_{\max}$) of a typical passive RFID system in the microwave band. The distance $r_{\max}$ refers to the maximum distance a tag can be placed to receive the necessary power from the reader. A part of this power supply uses the inner circuit of the tag to perform all the necessary operations to wake up the tag, and another part is used to transmit the data back to the reader. This distance is smaller than the actual reading distance due the attenuation in the reverse link.

By using the Friis relationship for the free space path loss given in equation 2.1 and the relationship between the transmitted power from the reader (P_r) and the power received by the antenna of the tag (P_{tag}), the one way (reader to tag) path loss (a_F) is given by:

$$a_F = \frac{P_r}{P_{tag}}. \tag{4.1}$$

Substituting P_{tag} with $P_{tag,\min}$, the next equation gives the maximum allowable path loss that the RFID system can experience for the tag to be capable of transmitting the stored data to the reader.

$$a_{F,\max} = \frac{P_r}{P_{tag,\min}}. \tag{4.2}$$

From equation 4.2, the maximum distance for a tag with a dipole antenna (most common in RFID), and a reader with maximum EIRP at the output of the reader's antenna equal to 4 Watts, was calculated and plotted in Figure 14.

Figure 14 illustrates the reading distance versus the transmitted power from a reader. It is $r_{max} = 3.5\,m$ and this result agrees with [17], which gives r_{max} up to $4\,m$ for a typical passive RFID system with data rates up to $30\,Kbps$ and also [2] gives the range of 3 m as the lower bound for backscattering RFID systems (UHF and Microwave bands).

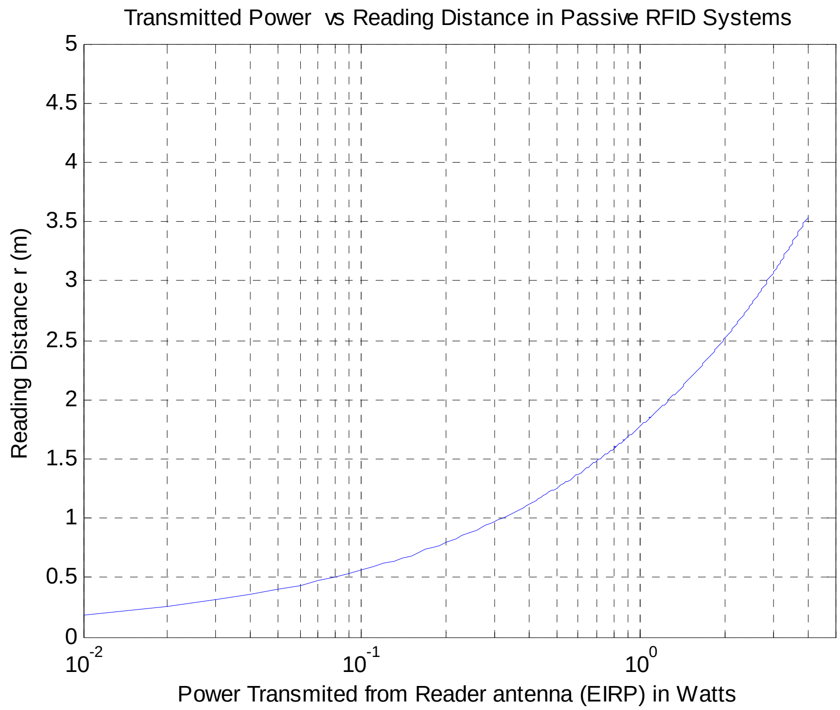


Figure 14. Reading Distance for a Typical Passive RFID System.

The results in Figure 14 are for Line-Of-Sight (LOS) communication between reader-tags, which is almost a prerequisite for microwave RFID systems.

If the RFID system is inside a building, for a line-of sight communication, the path loss exponent n (exponent of distance r) used in equation 2.1 is less than 2. Usually, a value of 1.6 to 1.8 is used for this case [18], and therefore, the maximum reading distance can be higher than that stated above.

To determine the maximum distance in an indoor environment, it is first necessary to compute the path loss a_F in a reference distance r_0 from the reader, using equation 2.1. Since the maximum distance for the free space was computed as $r_{\max} = 3.5\, m$, a reference distance $r_0 = 0.5\, m$ is selected, and $a_F(r_0 = 0.5) = 32\, dB$ is found.

The selection of the reference distance is not arbitrary for the RFID system and is determined as follows.

a. Evaluation of Reference Distance (r_0)

The reference distance r_0 could be any distance in the far-field region of the reader's antenna, which is much smaller than the maximum distance of this specific system [18].

It is known from antenna theory and design that the far-field distance or *Rayleigh* distance r_{ff} of the antenna is given by:

$$r_{ff} = \frac{2D^2}{\lambda} \tag{4.3}$$

where D is the maximum size of the antenna in meters. Any distance r, which meets the following requirements:

- $r > r_{ff}$,
- $r \gg D$, and finally
- $r \gg \lambda$

lies in the far–field region of the antenna.

Table 6 gives the *Rayleigh* distance r_{ff} for different types of reader antennas at 2.45 GHz ($\lambda = 0.1224m$). As can be seen from this table, for an antenna in the microwave band, the far-field region is determinated by the wavelength.

The selection of $r_0 = 0.5m$ (more than 4 times λ), satisfies the previous requirements and is eligible to be selected as a reference distance for the evaluation of the reference path loss from the Friis equation.

Type of Antenna	***Rayleigh*** **Distance r_{ff},(m)**	***Maximum Antenna Size D, (m)***
Dipole $\frac{\lambda}{2}$	0.061	0.061
Dipole $\frac{\lambda}{4}$	0.015	0.031
Patch with $D = 0.4\lambda$	0.04	0.049

Table 6. Rayleigh Distance for Different Antenna Types at 2.45 GHz.

b. Maximum Distance for RFID Systems in Different Environments

From the theory for the large–scale path loss at distance r, $a_F(r)$ is given in [18], by:

$$a_F = a_F(r_0) + 10\log(\frac{r}{r_0}) . \tag{4.4}$$

Using equations 4.1 and 4.3 and solving for distance r, the following relationship is found:

$$r = r_0 \times 10^{\left[\frac{\left(10*\log\frac{P_r}{P_{tag,\min}}\right) - a_F}{10*n}\right]} . \tag{4.5}$$

Figure 15 shows the maximum distance for two cases: for an indoor environment with path loss exponent $n = 1.6$, and for an urban environment with $n = 3$. Many times in applications such as the scanning of products in a store, the solid line ($n = 1.6$), is usually the case for the performance of the RFID system, and so greater ranges up to $5.5\,m$ can be achieved.

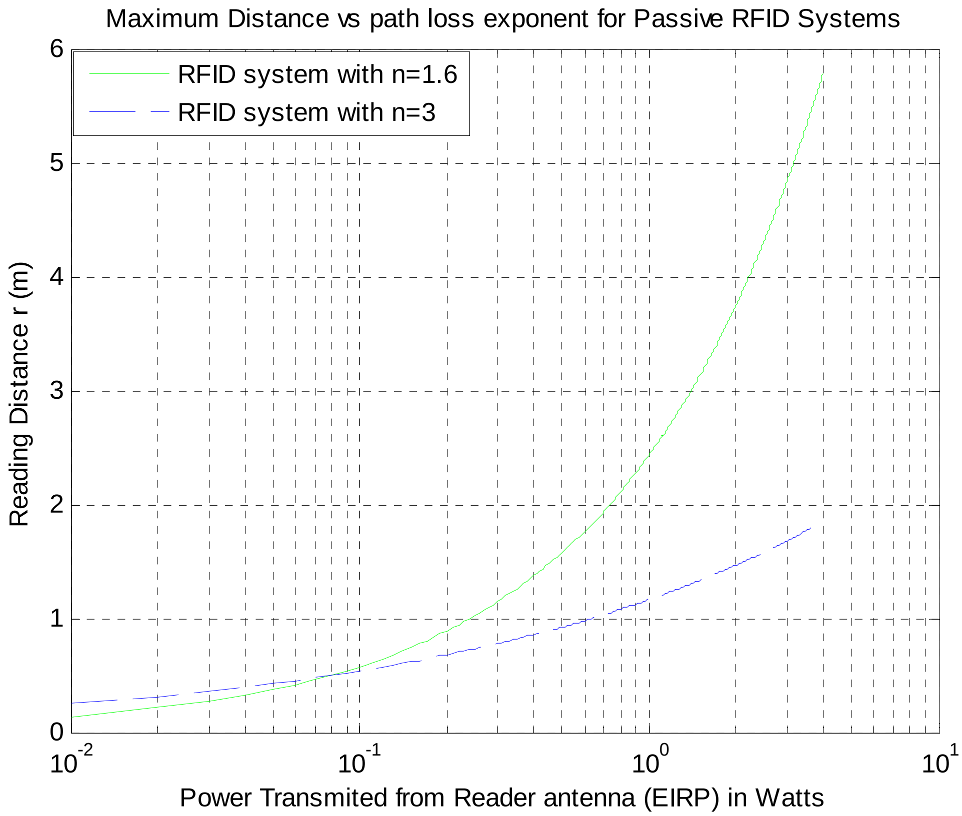


Figure 15. Maximum Distance for Different Values of Path Loss Exponent.

This figure illustrates the significant role of the environment in communications between the reader and tags due to the dependence on the reading range from it.

2. Selection of Backscattering Modulation at Tags

In passive RFID systems at the microwave band, the reader transmits the ASK modulated carrier to the shared wireless channel. This carrier provides the tag with enough power to energize it, and is also used by the tag as a carrier for transmitting its ID in the reverse link by using the backscatter modulation. The tag reflects the reader's signal by changing the impedance of its antenna according to the bits that are transmitting, or in other words, it changes the gain of the antenna [19, 20]. As a result, small fluctuations occur in the amplitude of the carrier's signal.

When the signal returns, the reader needs to "peak-detect" the modulation of the tag in the carrier and then decode it. A high value in the envelope of the carrier is

represented by a binary one '1' and a low value of a binary zero '0'. If this is the only change that occurs in the reader's signal, this type of backscatter modulation is called *direct* modulation and it is simply an ASK modulation. In addition, the tag can also change the phase or the frequency of the carrier signal, and thus, create a PSK or FSK modulated signal.

Figure 16 illustrates a direct modulated backscattering carrier signal from the tag to the reader. A carrier signal is an ASK modulated sine wave with amplitude $100\,V$. The tag creates a drop of $100\,mV$ in the amplitude of the carrier for each transmitted binary zero '0' [21]. The reader peak-detects this signal, decodes it and thus identifies the tag.

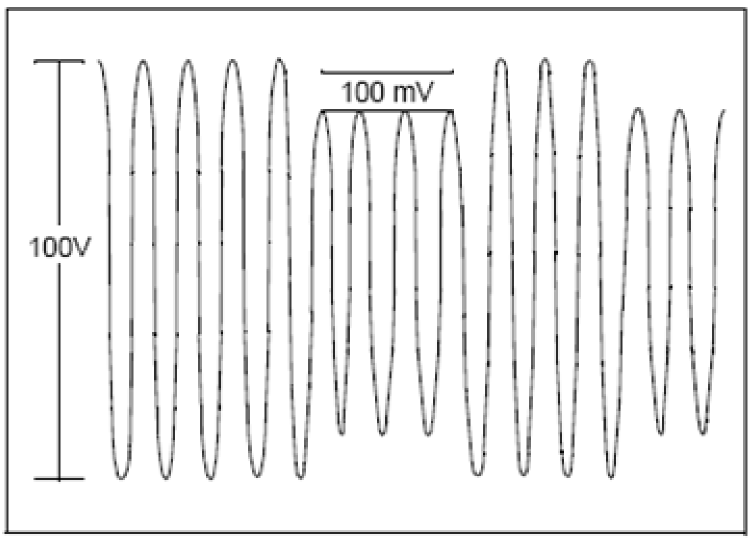


Figure 16. Backscatter Amplitude Modulation Signal (From Ref. 21)

For the case of passive RFID tags in the microwave band, this kind of ASK backscattering modulation is selected because of the simplicity either in detection from the reader and in computations inside the tags, which, as a result, reduces the cost of the tag. In addition, *direct* modulation (ASK) provides higher data rates (up to $40\,Kbps$) than PSK and FSK backscatter modulation [19, 21]. General passive tags must have as simple functions as possible to reduce the power consumption, and thus, to increase the maximum working distance of the RFID system [22].

Also, the messages transmitted from the tags must be as short as possible for two reasons:

- Shorter messages mean less power consumption in the tag.
- Shorter messages have lower probability of error in transmitting the tag's ID as discussed in the following paragraph.

a. Probability of Error in Transmitting Tag's ID with ASK Backscattering

When ASK is the only modulation (backscattering) used in the reverse link, then the Bit Error Probability (BER) P_b is given by (for coherent detection):

$$P_b = Q(\sqrt{\frac{E_b}{N_o}}) \tag{4.6}$$

where E_b/N_o is the average signal to noise ratio per bit and $Q(x)$ is the *Q*-function.

In the above expression, an *Additive White Gaussian Noise* (AWGN) channel with no fading is assumed.

The probability a bit is not in error is $P_n = 1 - P_\mathrm{r}$, and thus, the probability for a tag to transmit its ID without having any bit in error is given by:

$$P_F = \left(1 - P_b\right)^L . \tag{4.7}$$

In the above equation, L is the length in bits of the frame that the tag is using to transmit its ID, and is assumed to be the same for all tags.

Finally, the probability for a frame to be in error is given as:

$$P_{e,F} = 1 - P_F = 1 - \left(1 - P_b\right)^L . \tag{4.8}$$

Figure 17 illustrates the P_b for different values of E_b/N_o. Note that P_b becomes negligible for E_b/N_o greater than 7 dB (less than 1% error).

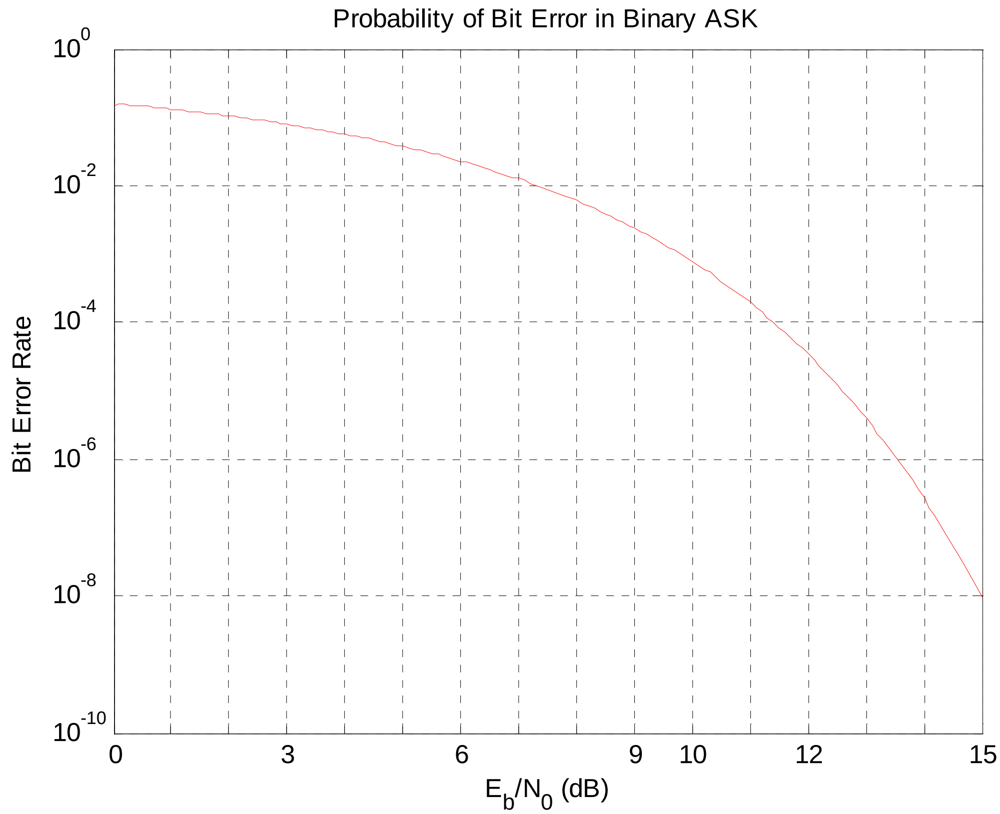


Figure 17. BER with ASK-Backscatter Modulation.

Equation 4.8 shows that shorter tag messages (smaller L) result in lower probability of frame error $P_{e,F}$, or in other words, a lower frame error rate.

Figure 18 illustrates the simulation of equation 4.8 for three frame lengths:

- $L = 64\,bits$, which is the minimum frame length from the ISO standards, and also is the length of the Unique Identification (UID) of the tag,
- $L = 144\,bits$, which is the recommended frame length from ISO standards, and,
- $L = 512\,bits$, which refers to the maximum frame length used in typical passive RFID systems.

It shows that for smaller tag messages, the frame error rate decreases, and moreover, for a 7 dB signal-to-noise ratio, the probability a frame is received in error is now significant (8×10^{-1} for $L = 144\,bits$).

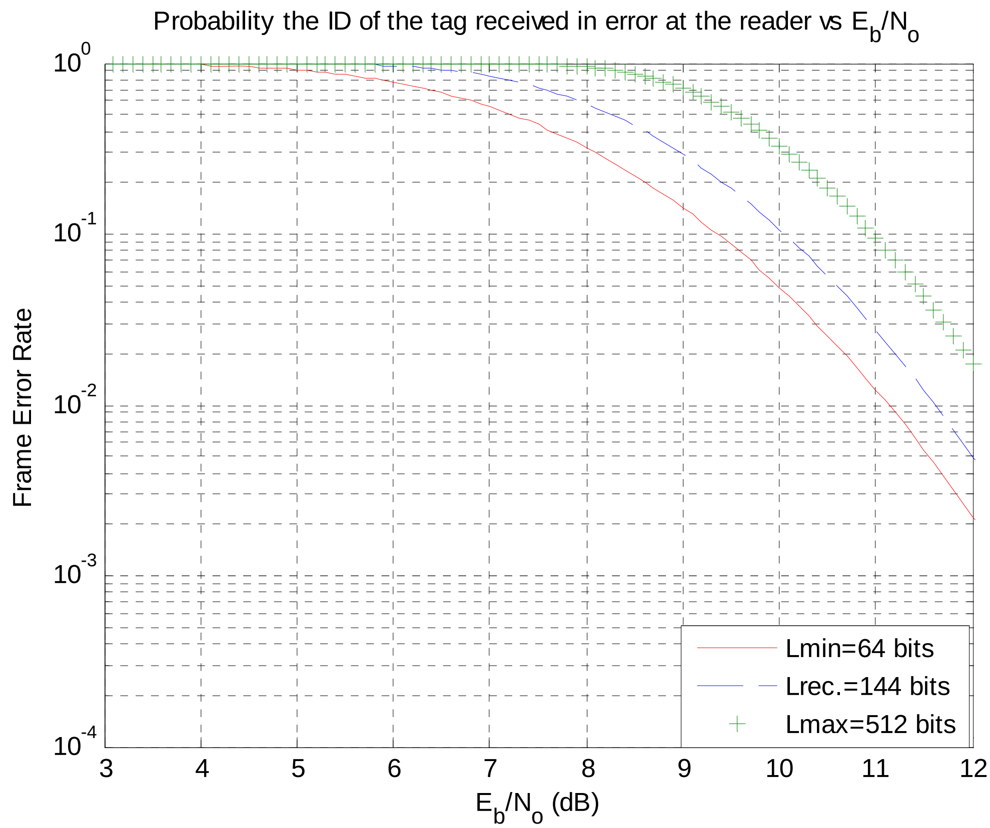


Figure 18. Probability the ID of the Tag Received in Error for Binary ASK Backscattering (Direct-Modulation).

Since only a 16 bit CRC is used for error detection and forward error correction coding is not applicable, it is very important to use short messages and for the signal received in the reader to be as strong as possible to reduce retransmissions and overhead in the reverse link.

b. Selection of Tags Frame Length

The format of the frame that the tag transmits to the reader (response) is given in Table 6, which shows the following fields [17]:

- Quiet. The tag does not transmit for a specific period of time determined from the protocol.
- Return Preamble. This consists of 16 bits in a specific sequence, which enables the reader to lock the data from the tag and start decoding the message.

- A 16 bit CRC for error detection.
- The data field with at least 64 bits for the UID plus the rest data bits to transmit other kinds of information stored in the tag's memory.

Quiet (0 bits)	Return Preamble (16 bits)	Data bits	CRC (16 bits)

UID (64 bits)	Rest Data bits

Table 7. Format of Tag Response (After Ref. 17)

Since it is important as previously mentioned to keep the tag's message as short as possible, but on the other hand, as error detection capability and the return preamble are necessary, a frame length of 96 bits is selected. However, the memory size of the tags can be larger (144 bits is the recommended standard), and thus it could be compatible even with the EPC (96 data bits).

Figure 19 shows the frame error rate for $L = 96$ bits. For a signal-to-noise ratio less than $11\,dB$, the frame error rate is still significant (7×10^{-1} for $7\,dB$). A signal to noise-ratio-greater than $11\,dB$ is necessary to achieve low frame error probability (lower than 10^{-2})

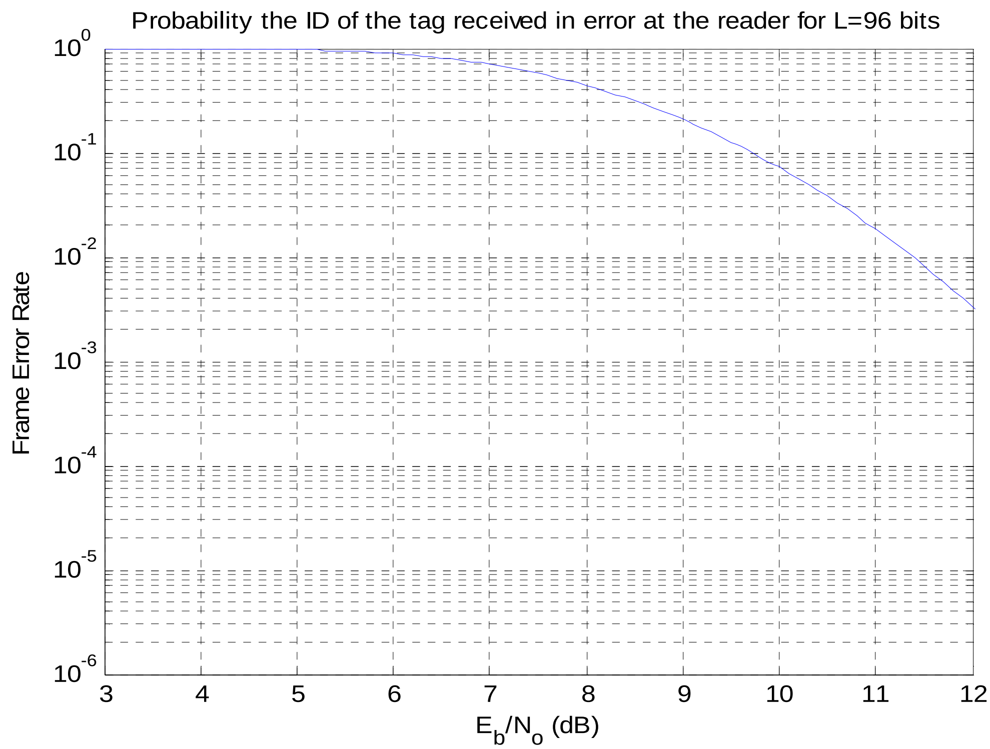


Figure 19. Probability the ID of the Tag Received in Error for Frame Length: L= 96 Bits.

Figure 19 is summarized in Table 8, which shows the frame error rate for different values of SNR.

Signal to Noise Ratio (dB)	**Frame Error Rate for L=96 bits**
2	Almost 10^{0}
5	Almost 10^{0}
6	0.9
7	0.7
8	0.4
9	0.2
10	0.06
11	0.02
12	0.003

Table 8. Probability the ID of the Tag Received in Error versus SNR.

3. Increasing the Efficiency in FSA with Capture Effect

The tag's responses in the reverse link can be identified from the reader even if they collide (occupy the same slot). This can happen if the strength of one signal is higher than the rest of the signals in the same slot. This is known as the *capture effect* [2, 18]. The capture effect is used very often in most common cellular systems.

For this thesis, it is possible to take advantage of the capture effect and increase the throughput S of the FSA algorithm by choosing the appropriate threshold in the reader, which acts as a filter for the weak signals. As a result, the reader identifies the tag even if collision has occurred in the specific slot.

The throughput S in the Slotted Aloha algorithm with the capture effect is given [23] by:

$$S = Ge^{(-\frac{TG}{1+T})} \tag{4.9}$$

where T is the selected threshold in the reader, which is called *capture ratio* and corresponds to how many times greater the received power in reader should be from a specific tag, compared to the summation of the received powers from the remaining tags that occupy the same slot in order to be identified by the reader.

Throughput S reaches its maximum value $S_{max} = \frac{1+T}{eT}$, when $G = 1 + \frac{1}{T}$, where T in above equations is given by: $T = 10^{\frac{T[in\,dB]}{10}}$.

Figure 20 shows that a higher throughput can be achieved in the RFID system by "filtering" the weak signals with the threshold T in the same slot and keeping only the survivor signal. It can be seen from this figure, that for a value of $T = 3\,dB$, throughput increases to $S_{3dB} = 0.552$ (for $G = 1.5$), and for $T = 6\,dB$, S increases to $S_{6dB} = 0.46$ (for $G = 1.3$).

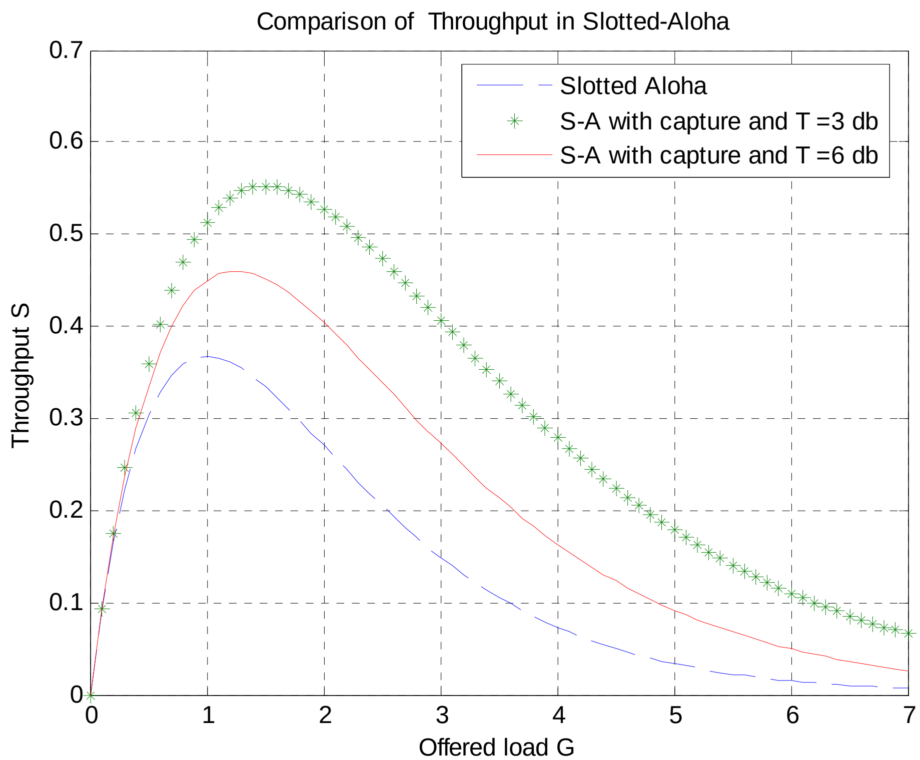


Figure 20. Throughput in FSA with the Use of Capture Effect.

So as T decreases, the performance of the RFID system increases, and as this takes place for higher values of G, so does the stability for the FSA algorithm. One could say that using a low threshold in the reader would eliminate the collision problem, but this cannot happen in practice, because T is determined by the reader's sensitivity.

The typical reader's sensitivity requires $6\,dB$ difference between the signal from the tag of interest and the channel noise (white noise plus interference from other tags) in order to identify the tag. Therefore, only an increase up to 46% in performance in terms of throughput can be achieved.

Table 9 shows the improvement for the Maximum Theoretical Throughput S in the FSA algorithm for different values of threshold T.

It is obvious that theoretically, even for very high values of T, such as $20\,dB$ (a cheap reader with very low sensitivity), performance is better than the maximum of the FSA algorithm without using filtering in the receiver of the reader.

Threshold T (dB)	**Maximum Theoretical Throughput S (%)**
2	59
3	55.2
4	51.4
6	46
7	44.1
8	42.6
9	41.4
10	40.5
15	37.8
20	37.15

Table 9. Maximum Theoretical Throughput for Different Thresholds.

4. Progressing Scanning Algorithm

The proposed PS algorithm considers two constraints of the RFID system:

- The power consumption in tags must be minimum in order for the RFID system to achieve the maximum distance, and
- The RFID system must be based in simplicity, especially for the tags.

a. Description

In the PS algorithm, the reader takes advantage of the range difference between the tags and the reader's antenna. Tags that are near the reader receive more power from the reader than those which are further away.

In the progressing scanning, the reader transmits starting from a minimum EIR power level $P_{r,\min}$ until the maximum $P_{r,\max}$ which is permitted from the regulations. Tags that are further from the reader do not receive enough power ($P_{tag,\min}$) and thus cannot transmit their IDs. In each retransmission, the reader increases the transmitted

power by an increment k and the tags that are further in distance reply. This continues until the transmitted power reaches $P_{r,max}$. Then, a new cycle begins and the procedure is repeated from the beginning.

The PS algorithm divides the number of tags n in the area into smaller groups as in the EDFSA algorithm introduced in [16], and therefore, this method has the benefits of EDFSA since the reader does not use large frame sizes that minimize the efficiency of Aloha-based algorithms [16].

Figure 21 illustrates how the PS algorithm works. In this specific figure, the distance $R_{\min}$ corresponds to transmitted power $P_{r,\min}$, and the distance $R_{\max}$ to the maximum transmitted power $P_{r,\max}$ (4 Watts).

A $P_{r,\min} = 1\,Watt$, and an increment $k = 1\,Watt$, were selected. Thus, the total numbers of tags were divided into four groups:

- The first group consists of the tags inside the circle with the center being the position of the reader and radius equal to $R_{\min}$ $(1.7733\,m)$.
- The second group contains all the tags in the area between $R_{\min}$ and $R_2 = 2.5078\,m$.
- The third group contains all the tags in the area between R_2 and $R_3 = 3.0714\,m$.
- The fourth and last group contains all the tags in the area between R_3 and $R_4 = 3.5465\,m$, which is the maximum distance for the LOS communication RFID system given by Figure 14.

It is assumed that tags from each previous group do not respond when the reader attempts to energize the tags in the next group.

The Cartesian coordinates x, y are in meters and $(x, y) = (0, 0)$ is the position of the reader. Finally, the negative values in the axes are meaningless, and are just for illustration.

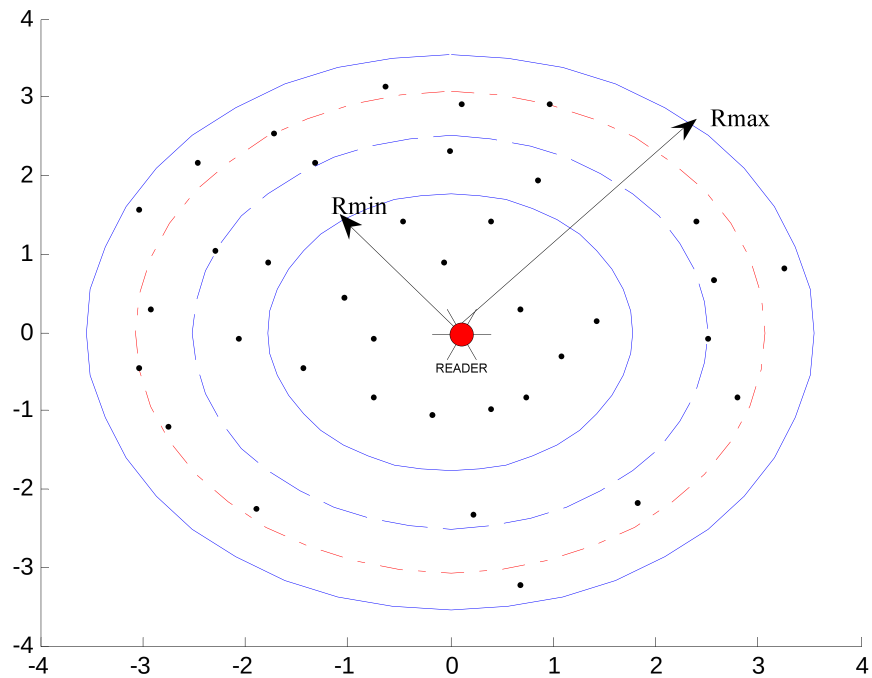


Figure 21. Example of the PS Algorithm, with Four Sub-Areas.

A detailed description of the PS algorithm follows:

- At first, the reader transmits with $P_r = P_{r,\min}$. The tags at distance $r_t \le r_{\max,p_i}$, (where $r_{\max,p_i}$ is the maximum distance of Figure 14 which corresponds to this transmitted power), become energized and reply using the FSA protocol.
- Next, the reader increases the power level by k, and the aforementioned procedure repeats, but now with transmitting power $P_r = P_{r,\min} + k$. All new tags that entered the interrogator zone of the reader reply. Tags from the previous scanning do not reply to the reader command. This can be accomplished if the reader transmits a command in the header that informs the tags, which have already transmitted once, not to reply until the next cycle. Of course, the tags need to have been programmed to do so. This programming can be done from the manufacture by using a flash memory in tags for quick loading to compare its state, or by using tags with Read/Write memory.
- This aforementioned procedure continues with $P_r = P_{r,\min} + ik$ $(\iota = 1,2,3...)$.
- Finally, in the last scanning, the reader transmits with $P_r = P_{r,\min} + i_{\max}k = P_{r,\max}$, where $i_{\max}$ is given by:

$$i_{max} = \frac{P_{r,max} - P_{r,min}}{k}. \quad (4.10)$$

- This is the end of the first cycle of the PS algorithm, which consists of $n+1$ transmissions. After this point, a new cycle with multiple scans begins and the whole procedure repeats until there are no more tags in the interrogation zone.
- The maximum frame size of the reader in each scanning will be that of Table 5 for EDFSA (256 slots).

The PS algorithm is an alternative and simplex method to divide the tags in the interrogation zone into smaller groups like in EDFSA, without any involvement from the tags. As a result, PS algorithm decreases the complexity of the tags. Thus, PS has all the benefits of EDFSA in the performance of the Framed Slotted Aloha.

Figure 22 shows that the PS algorithm successfully divides the tags in the interrogation zone into groups with a fewer number of tags.

For the simulation of Figure 22, 1,000 tags were randomly generated and uniformly placed around the reader with distances of $r = 0\,m$ to $r_{max} = 3.5\,m$. In addition, two different values of $P_r = P_{r,min}$ were used with different increments k.

The reason that more tags are in the first group for both cases is the result of the reverse proportional relationship between P_r and r. For example, for $P_{r,min} = 1\,Watt$, this corresponds to $r = 1.7\,m$ which is almost half the maximum distance. By increasing the transmitting power by a factor of 0.2 or 0.5 Watts, the increase in parameter r is almost insignificant; thus, fewer tags are included in the groups following the first one.

As Figure 22 illustrates, the number of tags in each group decreases as the minimum transmitted power from the reader $P_r = P_{r,min}$, and the increment k decreases. However, both smaller $P_{r,min}$ and k must, as a result, increase the times the reader needs to scan to identify all the tags in the interrogator zone, which thus, negatively affects performance in the PS algorithm as will later be demonstrated. On the contrary, if the number of tags is too high, small values of $P_{r,min}$ and k are needed to decrease the number of tags in each group.

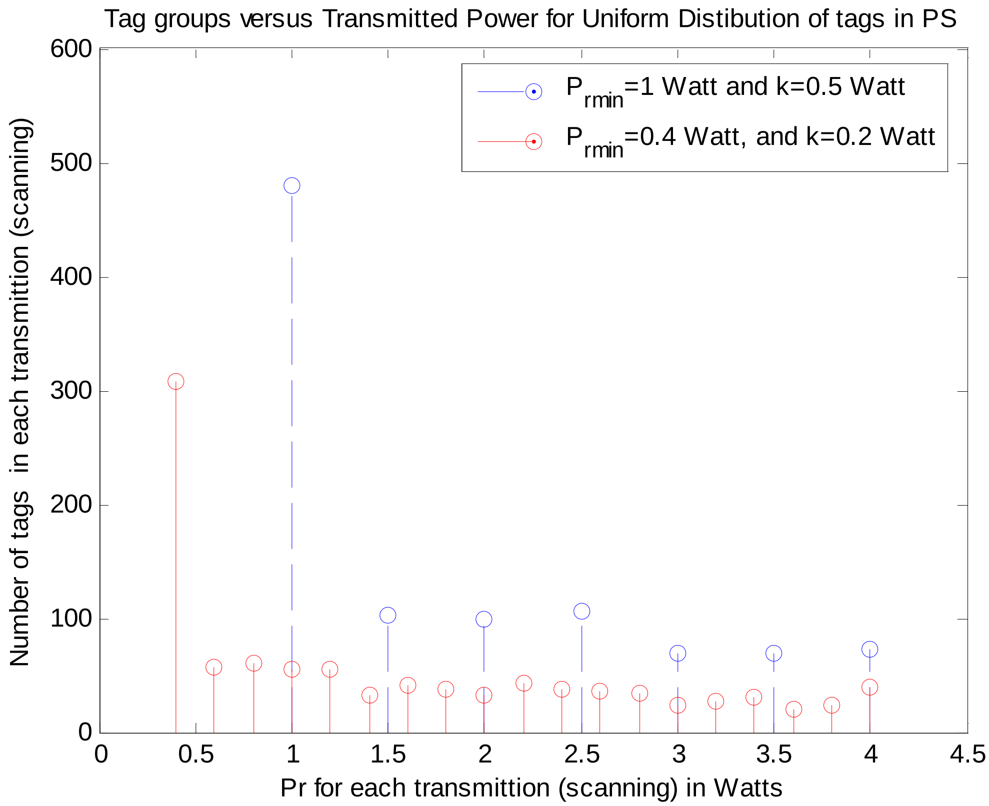


Figure 22. Groups of Tags in the PS Algorithm for Each Cycle for a Uniform Distribution around the Reader.

If instead of a constant value for the increment k, a variable one k_v is used, this will decrease the number of times the reader needs to transmit in one cycle. The only requirement is that this increment should increment while the transmitted power is increased, or in other words, smaller values of k_v should be used with the first scans where more tags are involved in the identification process and higher values when that transmitted reaches $P_{r,\max}$.

Figure 23 illustrates a comparison of the PS algorithm between a constant step $(k = 0.2)$, and a variable one $(k = \langle 0, 0.3, 0.9, 1.5, 2.5, 3.1, 3.6 \rangle)$. A uniform distribution for the range of tags around the reader was used again in this simulation.

The green solid line corresponds to a constant step and divides the tags into 19 groups, while the blue dashed line represents the variable step.

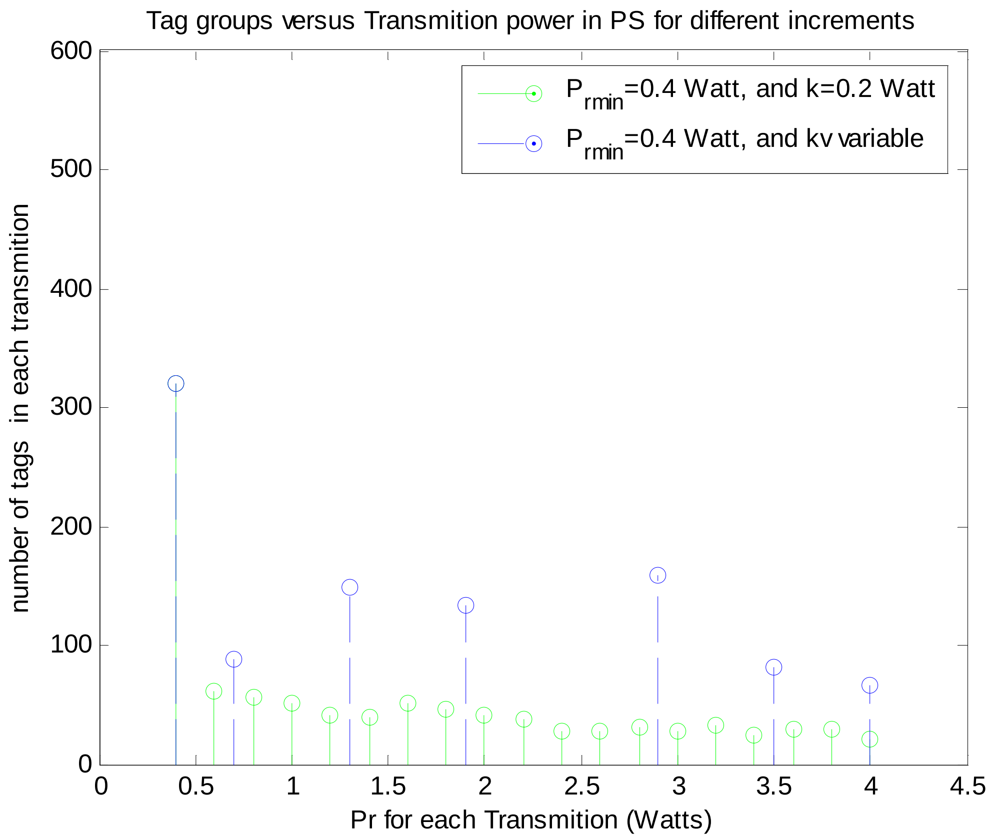


Figure 23. Comparison of Groups of Tags in the PS Algorithm for constant and variable step.

As seen in Figure 23, an increasing variable step decreases the number of scans of the PS algorithm, which has a similar effect if a higher constant value for k was used. Generally, a variable step can be avoided because it increases the complexity of the system. However, when the distribution of tags is different from the norm, it might be useful. For example, if the tag's distance from the reader follow a Gaussian distribution, smaller increments can be used near the mean distance and larger ones for tags that are many standard deviations greater.

b. Comparison between FSA and Progressing Scanning Algorithm

In order to compare the performance of the PS algorithm with FSA, it is necessary to simulate in discrete time using Matlab as the frame transmitted from the reader and also the random selection of a slot from the tags.

A fixed frame size is used both for the FSA and PS algorithms. The distance r of the tags from the reader is assumed to follow the uniform distribution with $r_{min} = 0\,m$, and $r_{max} = 3.54\,m$, which is the maximum distance for an outdoor line of sight RFID system at a frequency of $2.45\,GHz$.

The number of tags n in the interrogation zone is 1,000 and the simulation is ran 1,000 times to increase the accuracy of the results. The scope of the simulation is to evaluate the performance in terms of the time delay T needed for the identification of all the tags.

The time delay T for FSA in terms of the number of slots is given by equation 3.12, rewritten for convenience as $T_{FSA} = \frac{N}{(1-\frac{1}{N})^{n-1}}$. Thus, the delay in units of *seconds* is given by the following equation:

$$
\begin{aligned}
T_{FSA} &= \frac{N}{(1-\frac{1}{N})^{n-1}}\left[slots\right]*\left(\frac{L\left[bits/slot\right]}{R\left[bits/\sec\right]}\right) \Rightarrow \\
T_{FSA} &= \frac{N}{(1-\frac{1}{N})^{n-1}}*\left(\frac{L}{R}\right)\left[\sec\right]
\end{aligned}
\tag{4.11}
$$

where:

- L is the length of the tag response in bits (Optimal $L = 96$ is selected).
- R is the bit rate from the ISO standards (a minimum $R = 30\,Kbps$ is selected).

To calculate the delay from equation 4.11 for the PS algorithm, it is important to understand that the PS algorithm is just a FSA procedure with the only difference being that the number of tags n in the interrogation zone is divided into multiple groups. The delay for each group which contains n_i tags is given then as:

$$T_{PS_i} = \frac{N}{(1-\frac{1}{N})^{n_i-1}}*\left(\frac{L}{R}\right)\left[\sec\right] \tag{4.12}$$

where i indicates the number of groups, and n_i is the number of tags in this group that the PS algorithm has created. For example, for Figure 21, where the PS algorithm divides the interrogation zone into four areas, $i = [1,2,3,4]$.

Thus, the total delay T_{ps} in seconds of the PS algorithm is the summation of the individual delays for each group, and is given by:

$$T_{PS} = \sum_{i=0}^{i_{\max}} \left(\frac{N}{(1-\frac{1}{N})^{n_i-1}} \times \left(\frac{L}{R} \right) \right). \tag{4.13}$$

This average total delay does not include the time in which the reader needs to temporally inactivate the tags after identification. Such omission is also done for FSA, which is represented by equation 3.12. Since the time to inactivate the tags for both FSA and PS algorithms is the same, comparing the performance of PS to FSA using equations 4.13 and 3.12 is fair.

For $\mathrm{P}_{\mathrm{r,min}} = 0.2\,Watt$ and a step of $k = 0.2\,Watt$ ($i_{\max} = 18$) the PS algorithm was simulated and the results are showed in Table 10. The third column of this table shows how many times (power levels) the PS algorithm needs to transmit to complete one cycle, while the fourth column shows how many tags were identified in the first cycle. Finally, the last column gives the average time delay calculated from equations 4.12 and 4.13 for each case (except for FSA with $N = 64$ and $N = 128$ slots, which is from the simulation).

The results indicate that when a small frame size is used ($N = 128$ or $N = 64$), the performance of the PS algorithm is much better than that of FSA, which is unable to identify such a large number of tags due to collision. Moreover, the time delay introduced by the PS algorithm is reasonable (7-10 seconds for 1,000 tags).

When a larger frame size is used ($N = 256$), the PS algorithm is able to read more tags in the first cycle than can FSA with a greater frame size, but more

transmissions occur than in FSA. In addition, the average time delay T is much lower in the PS algorithm than in FSA (56% lower), and thus, the PS algorithm rapidly increases the performance of Slotted Aloha in terms of identification time.

Algorithm	**Frame Size (slots)**	**Number of scanning per cycle**	**Number of Tags Read in First Cycle**	**Number of cycles needed for the identification**	**Average Time Delay T in secs**
FSA	512	1	140	17	11.6
FSA	256	1	20	29	40.9
PS	*256*	*19*	*336*	*2.5*	*17.9*
FSA	128	1	0	Ineffective. Too many tags	∞
PS	*128*	*19*	*275*	*Less than 4*	*10.3*
FSA	64	1	0	Ineffective. Too many tags	∞
PS	*64*	*19*	*250*	*4*	*7*

Table 10. Comparison of FSA Algorithm versus PS Algorithm with $n = 1000 tags$, and $i_{\max} = 18$ (19 Power Levels).

It is important to notice from the results of Table 10 that for this specific simulation, while FSA is ineffective in identifying the entire number of tags in the area for the small frame size, the PS method with the same frame size provides a very low average identification time even compared with a PS with a larger frame size.

In Figure 24, the average time delay T is plotted for both the FSA and PS algorithms for frame size $N = 256\,slots$. For the PS algorithm, the structure of Table 10 was used with $P_{r,\min} = 0.2\,Watt$ and $i_{\max} = 18$. The simulation was run for the number of tags n from 100 to 4,000.

For a better presentation of the results, a linear scale was used for the horizontal axis (T), while a logarithmic scale was used for the vertical axis (number of tags).

From the comparison between the FSA and PS algorithms from Figure 24, the superiority of the proposed PS algorithm when compared to FSA is obvious when the number of tags in the area is too high; For example, for 4000 tags, it is $T_{PS} < 30\,\text{sec}$, and $T_{FSA} > 120\,\text{sec}$, respectively. However, when the number of tags is less than 790, the average delay is lower for the FSA algorithm, and thus, FSA performs better.

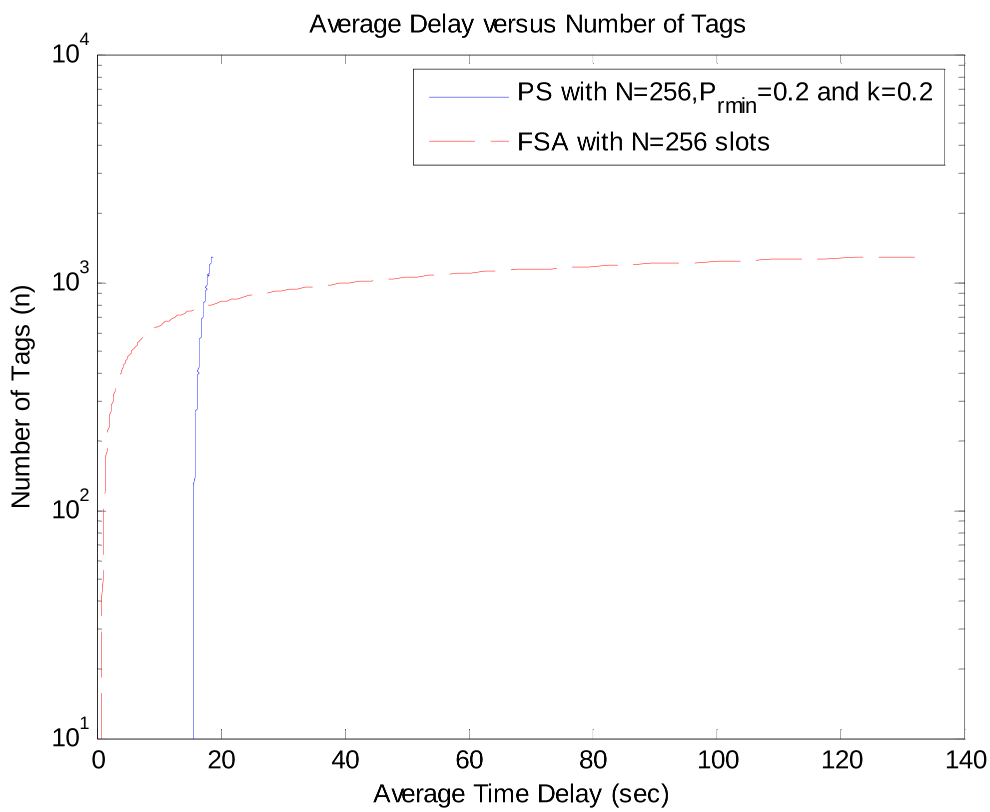


Figure 24. Comparison of Performance (Delay) between FSA ($N = 256$ slots), and PS ($N = 256$, $i_{\max} = 19$).

Figure 25 more distinctly shows the variation of the average delay with the number of tags for the PS algorithm. This figure shows that T increases very slowly

while the number of tags increases. This was expected because the PS algorithm uses 19 power levels and thus divides the tags into 19 groups. Therefore, an increase of $10-20$ tags does not affect it since those tags are mapping in 19 groups and not just one group (as in FSA).

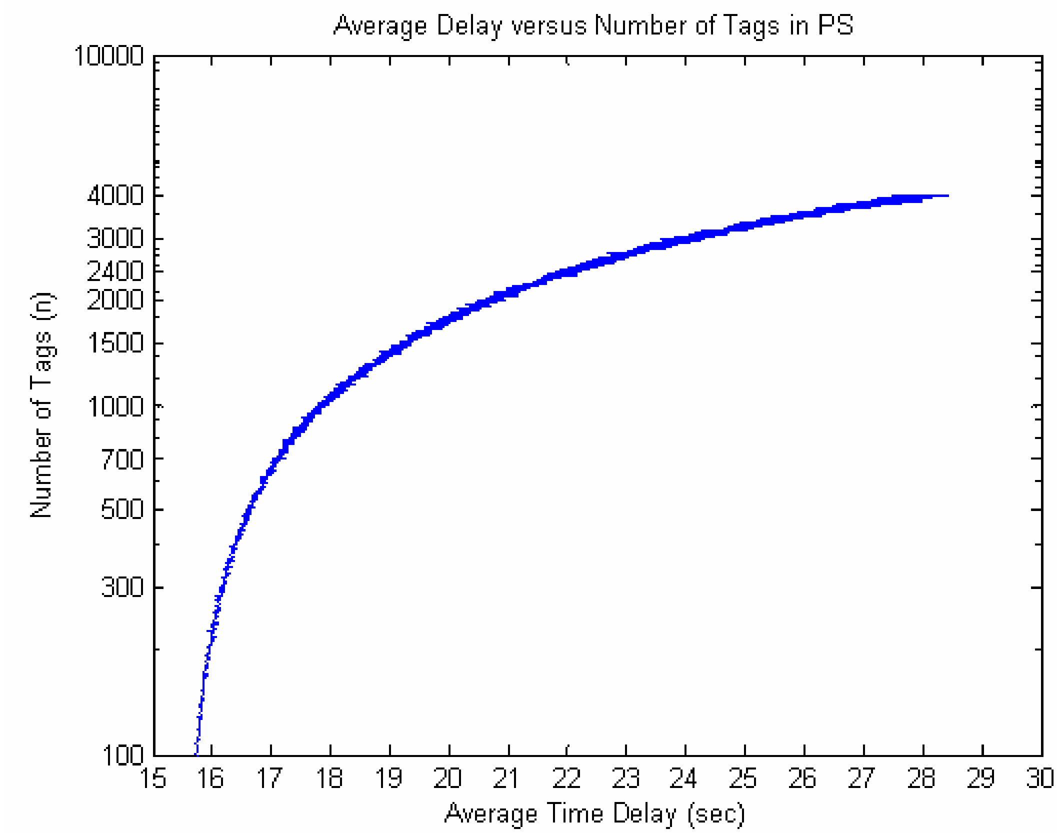


Figure 25. Delay T in PS versus Number of Tags for Table 10.

The problem with the PS algorithm is the high value of the initial delay (for 100 tags). This might occur because the PS algorithm transmits 19 times instead of only one time, and also after the first cycle, the reader needs to transmit again in all those different power levels corresponding to different distances (and tag groups) from it, even if some of those groups do not contain any more tags.

The results of Table 10 demonstrate that for $n = 1000$, a smaller frame size in the PS algorithm results in a lower average delay T. Thus, an answer to the high initial delay of the PS algorithm is to use a lower frame size.

Figure 26 illustrates the positive effect of a smaller frame size in the delay in the PS algorithm. Two different frame sizes ($N = 256$ and $N = 64$) were used for Table 10. The results show the beneficial influence of the smaller frame size for the number of tags n up to nearly 2760 tags.

However, a number of 2760 tags is a big number. Normally, in most applications, the number of tags does not reach this number. For this reason, in most of the simulations, the authors use up to 1,000 tags. As a result, a smaller frame size is the best choice when the PS algorithm is used.

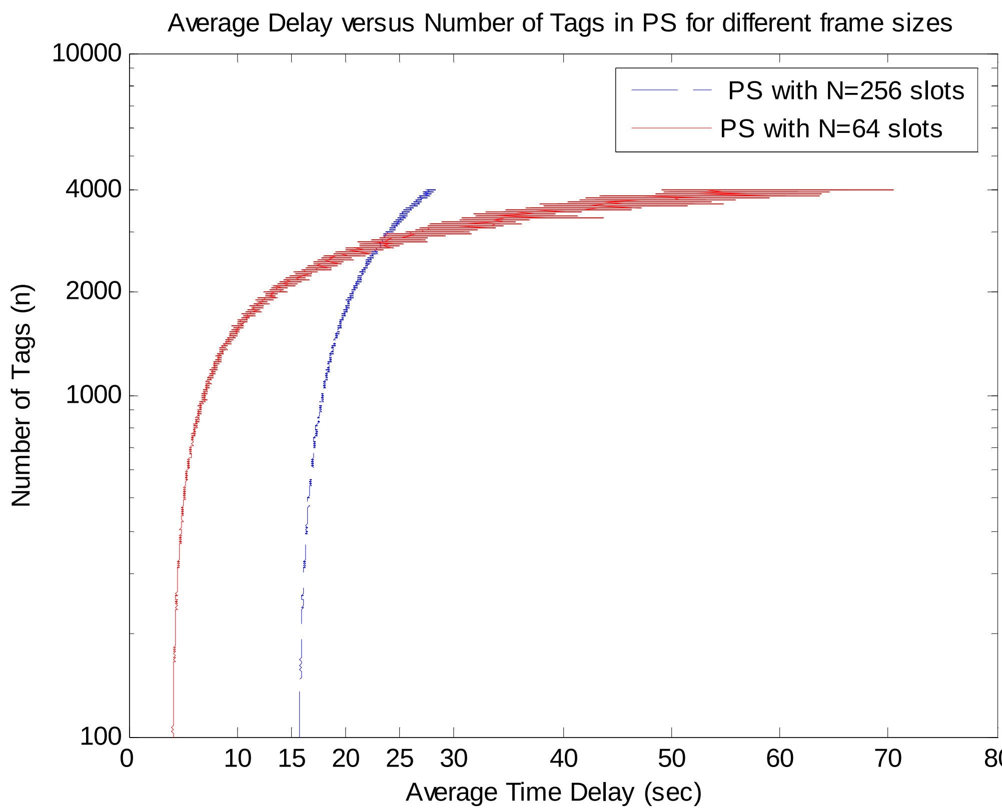


Figure 26. Comparison of Delay in PS for Different Frame Sizes $\left(N = 256 \textit{ and } 64 \textit{ slots}\right)$ for Table 10.

Figure 27 summarizes all the above cases for a better comparison in a two dimensional plot. The blue line with the cross symbol (+) represents the PS algorithm with $N = 64$ slots. This figure shows that using a smaller frame size in the PS algorithm is not only superior than using a larger frame size in the PS algorithm, but it is also the

best choice as compared to FSA with a larger frame size. However, because of the initial delay that the PS algorithm introduces (due to multiple scans), it has a lower performance than the FSA for a small number of tags in the interrogation zone (less than 480 in that case).

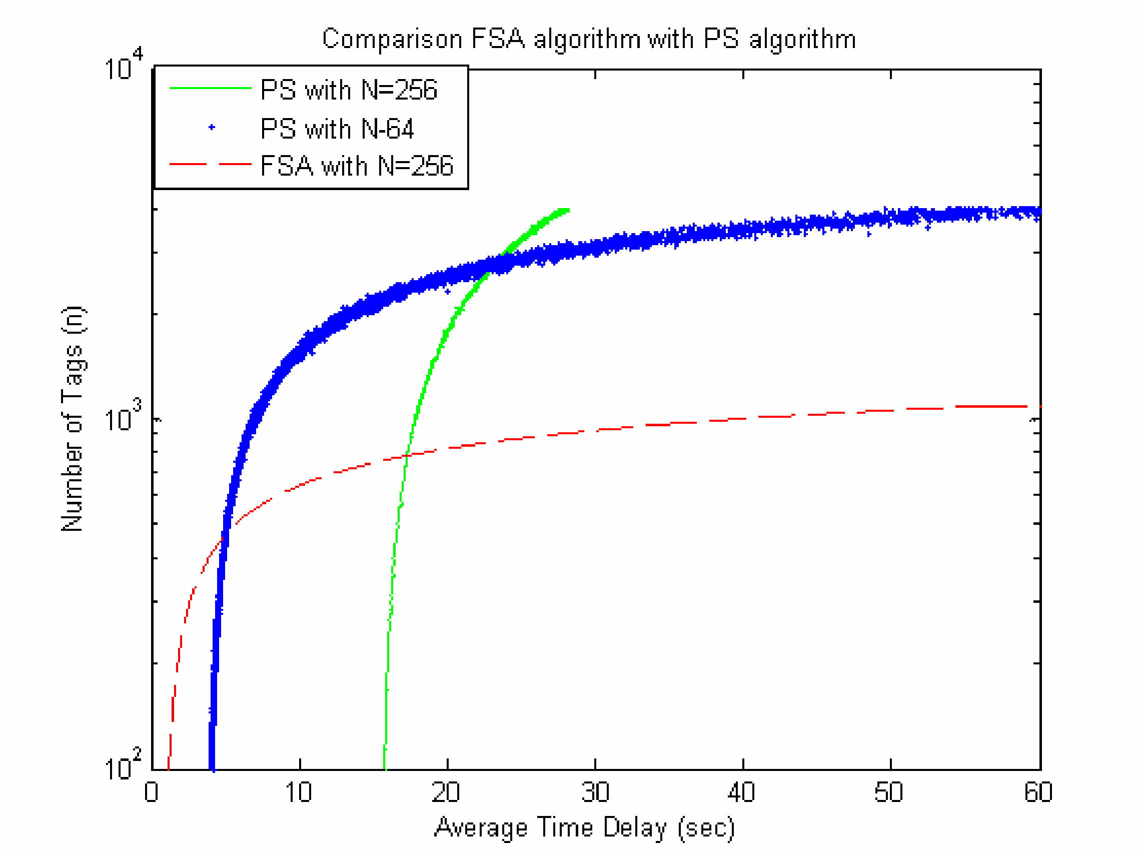


Figure 27. Summary and Comparison of Delay in PS $(N = 256 \text{ and } 64 \text{ slots})$ and FSA $(N = 256 \text{ slots})$ for Table 10.

Furthermore, as Figure 28 illustrates, the PS algorithm performs better when choosing a larger step equal to 0.4 Watts, which means that the tags are divided into fewer groups than before.

In this figure, both PS algorithms have a smaller initial delay and exceed the performance of FSA sooner (at 338 tags for the case of $N = 64$). On the other hand, when the number of tags is increased too much, the PS algorithm is outperformed compared to the previous case, where a step equal to 0.2 Watts was used.

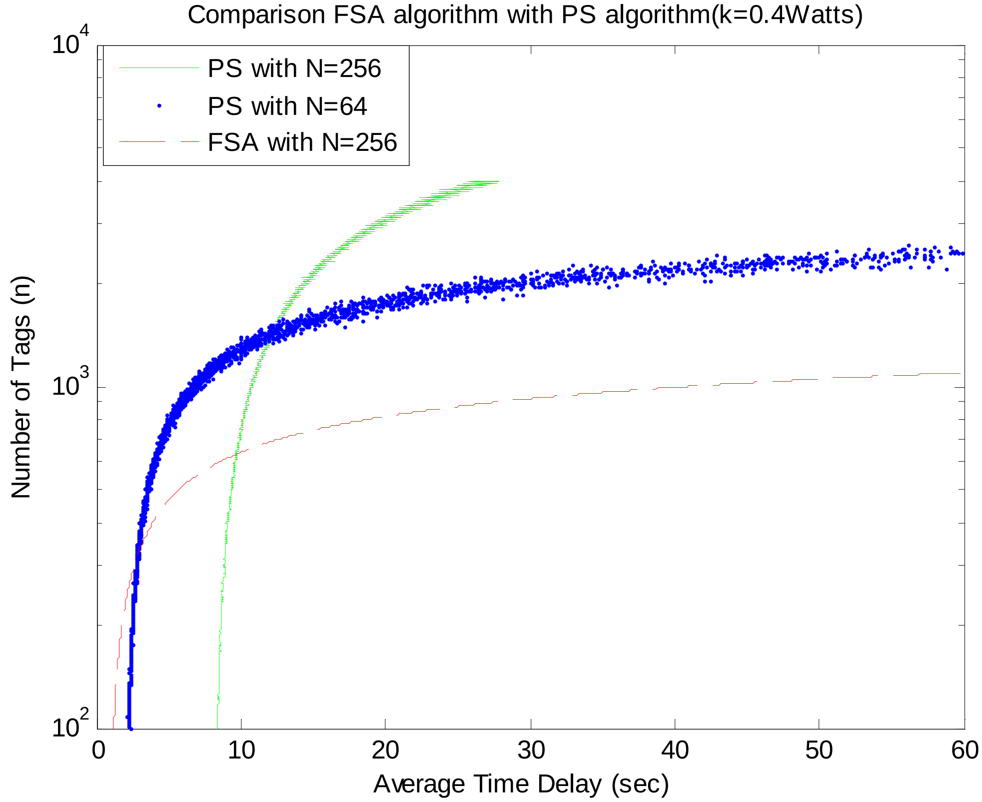


Figure 28. Comparison of Delay in PS $\left(N = 256 \; and \; 64 \; slots\right)$ and FSA $\left(N = 256 \;\; slots\right)$ for Table 10.

c. Comparison

As observed from the plots of the previous paragraph, the effectiveness of the PS algorithm against the FSA is not always the same but depends on the following variables:

- The selected frame size of the reader N.
- The increment (step) k in watts is used by the reader, and determines the number of scans in each transmitted cycle.
- The minimum transmitted power $P_{read,\min}$, also determines the number of scans in each transmitted cycle as well as the effectiveness of the algorithm in the first scan.
- And finally the number of tags n in the interrogation zone.

To evaluate the performance of the PS algorithm in terms of the average time delay, and to observe how this performance is affected by the number of tags in the interrogation zone, the step size and the frame size, the PS algorithm is simulated and creates three-dimensional mesh plots as illustrated in Figures 29 to 32..

In the simulation that results in the following figures, the minimum transmitted power $P_{read,\min}$ is assumed constant and equal to 0.4 Watts, and also, either the frame size or the step is kept constant, depending on which plot is referenced.

Figure 29 shows the performance of the proposed algorithm for the different frame sizes of 32, 64,128, and 256 slots. The step of increasing the transmition power of the reader is constant and equal to 0.2 Watts, and the number n of the tags is increased from 100 to 2000.

The horizontal axis y represents the number of tags in the interrogation zone, while the axis x represents the selected frame size. Finally, perpendicular to the xy plane, the z axis gives the average time delay for the PS algorithm.

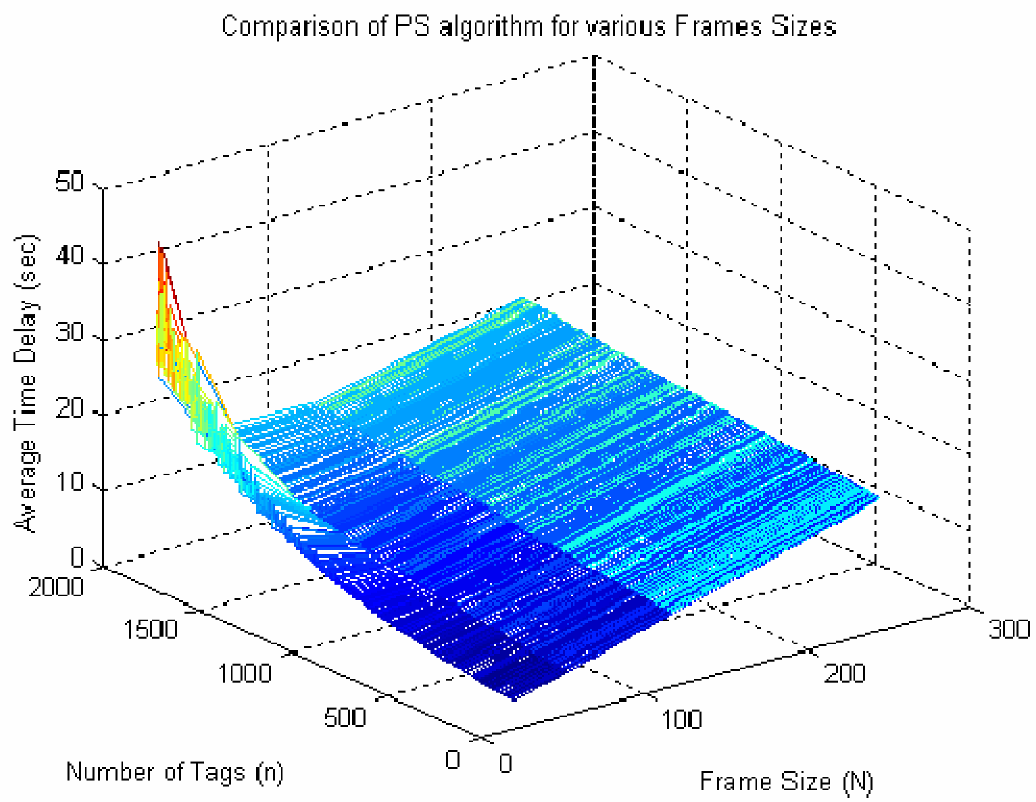


Figure 29. Performance of the PS Algorithm with Frame Size ($N = 32, 64, 128, and\ 256\ slots$) and Constant Step ($k = 0.2\,Watts$).

As Figure 29 shows, the slope of the mesh plot with the Y axis is smaller for a smaller frame size and increases while the frame size increases. That means the initial delay is higher when a large frame size is used by the reader, and the tags in the area are just a few. This was expected since the reader needs more time to transmit the larger frame and it also waits longer for the response from the tags.

Moreover, the average time delay is increased with the higher rate for the smaller frame size than the larger, while the number of tags is increased. This was expected as well, due to the increasing number of collisions which occurs when a small frame size is used. It is easy to observe that for the maximum number of 2000 tags, the frame size of 32 slots has a delay of over 40 seconds, twice that for the 256 slot frame size. However, with 100 tags at the beginning of the simulation, this frame size is the most efficient.

Figure 30 reproduces the previous figure with some data points that prove the aforementioned conclusions. The selected points of the graph were for 1000 and 1638 tags. As Figure 30 illustrates for the case of 1000 tags, the average time delay is less when a frame size equal to 32 slots is selected ($6.53\sec$) as compared to $64, 128$, and 256 slots, and thus, the performance of the PS algorithm is higher. On the contrary, when the number of tags in the interrogation zone is approximately 1638 tags, the best average time delay is with a frame size equal to 64 slots ($11.01\sec$), and thus, the performance of the PS algorithm is now higher for this frame size than the one of 32 slots.

The above results show that the performance of the PS algorithm is closely related to the existing number of tags as in the FSA algorithm. Therefore, it is very important for the reader to estimate the number of tags before the next cycle, as in DFSA.

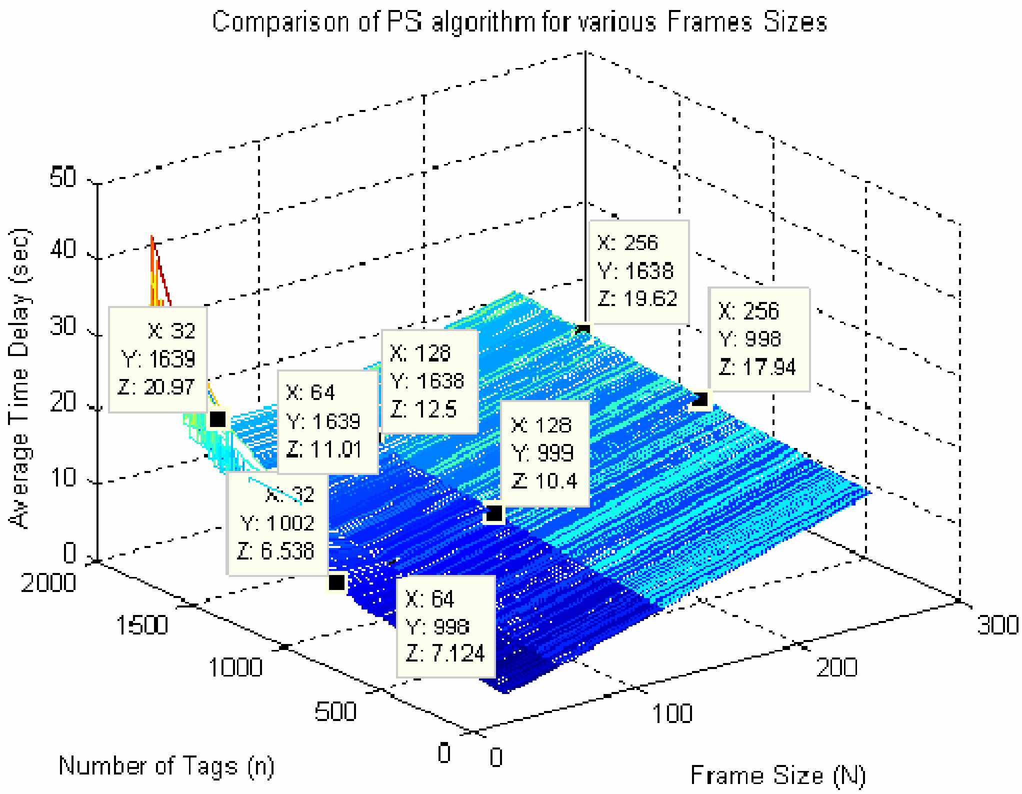


Figure 30. Data Points Demonstrating the Performance of the PS Algorithm regarding the Number of Tags for Various Frame Sizes.

Figure 31 shows the performance of the proposed algorithm when the step increasing the transmission power of the reader is not constant. The values for k equal to $0.2, 0.4, 0.9$ *and* 1.8 Watts are selected, while the frame size is constant and equal to 128 slots.

In this three dimensional mesh plot, the Y axis represents the number n of the tags, and the X axis the different steps used. The vertical Z axis once again gives the average time delay of the algorithm.

The first subplot has a maximum number of tags in the interrogation area equal to 1000, while in the second subplot, the maximum number of tags is 2000. This was done for better presentation of the results when the number of tags is increased rapidly.

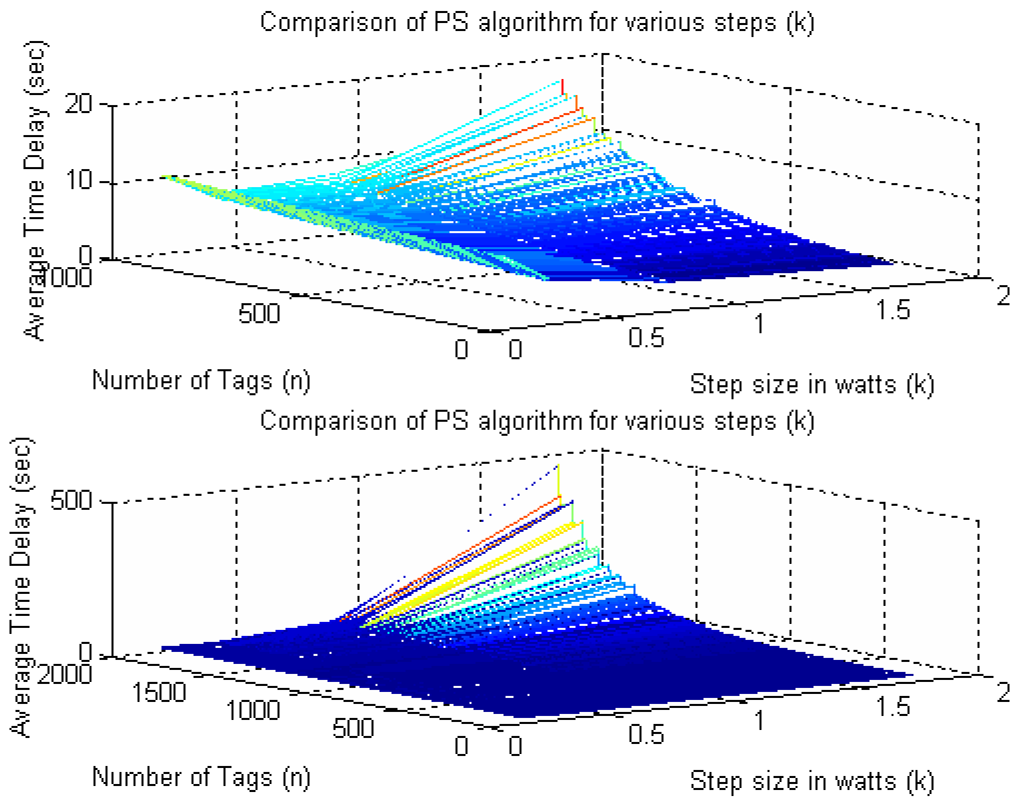


Figure 31. Performance of the PS Algorithm regarding the Step Size ($k = 0.2, 0.4, 0.9, and\ 1.8\ Watts$), and $N = 128\ slots$.

The second subplot of Figure 31 easily shows that when the number of tags is too high, the average time delay is increased rapidly when a large value for the step is used; thus, the performance of the PS algorithm decreases. This inverse proportional relationship between the delay and the step size is logical, because when a large value for the step is used, then the PS algorithm is almost the same with the FSA algorithm, and thus, in order to identify a large number of tags, more time is needed due to collisions, or to increase the frame size as in DFSA [11, 16].

In the first subplot, it is more obvious that the step affects the performance of the PS algorithm regarding the number of tags in the area. If the tags are only a few, a higher step is better, and actually as shown in Figures 26 to 28, the FSA is even better.

However, when the number of tags is increased, smaller steps result in less delay. In this subplot, the step of 0.4 *Watts* generally seems to result in better performance for the PS algorithm.

To better observe the results, Figure 32 is simply the first subplot of Figure 31, in which some data points were added. The data points show the previous comments about Figure 31, and especially the inverse proportional relationship between the step size and the average delay when the number of tags is increased, or more precisely, for few tags in the area, i.e., 427 tags, a higher step of 1.8 *Watts* provides the best results for the PS algorithm, while for the larger number of 1000 *tags*, the step size of 0.4 *Watts* results in better performance for the RFID system.

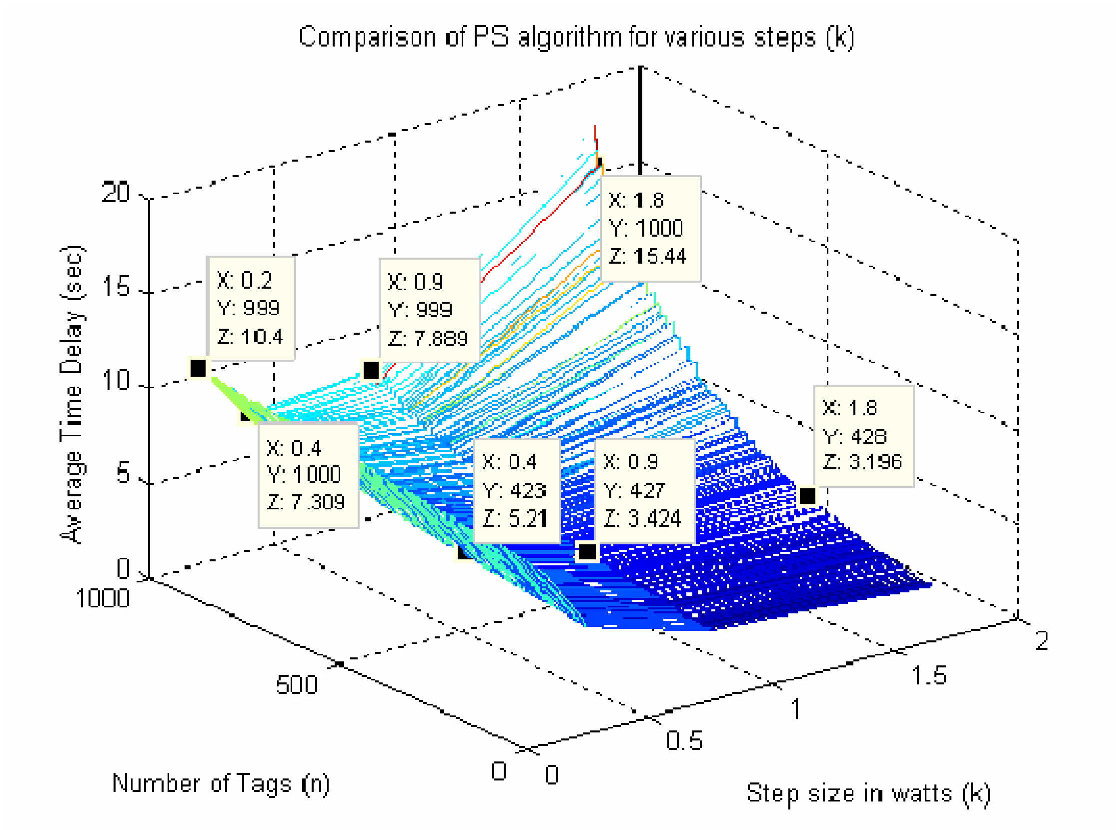


Figure 32. First Subplot of Figure 31 with Data Points at Y=427 Tags, and Y=1000 Tags.

All the above results from the simulation (Figures 29 to 31), indicate that in order for the proposed algorithm to be effective, it is important to select the right frame size as in DFSA as well as the right step. To do so, it is essential to know the number of tags inside the interrogation zone as this mainly affects performance and is closely related to the other two variables.

Since the PS algorithm is more effective than the simple FSA when the number of tags in the interrogation zone of the reader is high, only in that case is it necessary to implement it. Thus, the selection of the step size is simple. It must be small enough ($0.2-0.4$) to divide the tags into many small groups in order for the reader to be able to identify them using the Aloha algorithm. The exact value of k depends on n and also the selected frame size.

For the case of the right frame size, it is essential for the reader to have a good estimation of the number of tags n .This is the main problem from which both DFSA [11] and EDFSA [16] also suffer.

The simplest estimation can be provided by the lower bound of equation 3.13, which is rewritten here for convenience:

$$N = R + 2C \,. \tag{4.14}$$

After the first cycle of transmissions, the reader calculates the frame size N, by counting the tags that identify, given by R, and the collisions that occur, given by C. This bound should work better for the PS algorithm since the number of collisions in each scanning is less than in FSA or DFSA using the same frame size, because the number of tags is not as great as in those algorithms.

Moreover, another more complicated method to estimate the number of tags n in the area is provided by [11], where the authors proposed two formulas in order for the reader to do so. The first is given by equation 4.15, and is called the "Tag Estimation Method I":

$$C_{ratio} = 1 - (1 - \frac{1}{N})^n \, (1 + \frac{n}{N-1}). \tag{4.15}$$

N is the frame size used in the previous round from the reader, and C_{ratio} is the collision ratio (C/N), which is known after the first round/cycle.

The second is given by equation 4.16 and is called "Tag Estimation Method II":

$$n_{est2} = 2.3922 * C . \tag{4.16}$$

C is again the number of slots with collision.

All the aforementioned equations 4.14 through 4.16 will provide an estimated number for the tags in the area, and thus, the reader can select the appropriate frame size for the PS algorithm, which is the same as in DFSA (equal to the number of tags).

Chapter V presents some of the most important applications of the RFID systems together with a proposed application for *Information Warfare*. The large number of current applications for RFFI systems shows the how important it is for the reader to be able to collect the data from the tags with high integrity, and this is precisely what the PS algorithm does.

V. APPLICATIONS OF RFID SYSTEMS

A. GENERAL APPLICATIONS OF RFID SYSTEMS

RFID systems can provide real time information, high accuracy in data transfer, and in most applications, line of sight is generally not required. In addition, RFID systems that operate in higher frequency bands provide high data rate capabilities both in reading data from the tags, and also in writing data to them. All of the above are accomplished with fully automated mechanisms and low human participation. As a result, they are preferred to barcodes, biometry, and smart cards. Operating frequency is an important parameter of the RFID systems.

1. Frequency and RFID Applications

A variety of applications use RFID systems. The operating frequency of the system is one of the most important factors that must be considered before selecting a RFID system as many properties of this system depend on the operating frequency.

Table 11 shows the main frequency bands for RFID systems [2, 4] and some applications and comments about each band. Most importantly, at the frequency of 2.45 GHz, the RFID system can achieve high data rates with the use of very small size tags, which can reduce the cost of the RFID system and also provide a large amount of information in real time.

A major obstacle for the RFID systems (regarding the operating frequency) in the microwave band is that the standards are not well established and are still being constructed. The ISO is a step ahead, and has published most of them.

Frequency Band	Applications	Remarks
Low Frequency (100-200 KHz)	• Access control and time recording • Livestock tracking (Animal Identification) • Automobile antitheft systems	• Large size of tags • Low interference with metal • Low read range
High Frequency (3 -30 MHz)	• Public Transportation • Baggage tracking • Access control	• Better anticollision and increased memory capabilities than UHF RFID systems. • Serious interference with metal • Low read range
Ultra High Frequency (850 -950 MHz)	• Supply chain (pallet and container tracking)	• Balance between path loss and tags size, with less cost than HF tags. • Affected by moisture • Large read range
Microwave (2.4 GHz- 5.8 GHz)	• Logistics and roadway systems.	• Smallest size tags • Higher data rate • Higher path loss than any other RFID system, but greater read range than other standards.

Table 11. General Applications of RFID Systems regarding the Frequency Band.

2. Tracking Goods and People with RFID Technology and the PS Algorithm

A list of the most important applications of RFID technology where a microwave RFID system could be used is a follows:

- People Identification
- Toxic Waste Monitoring
- Animal Identification
- Asset Management

- Parts Identification
- Food Production Control
- Toll Collection
- Stolen Vehicle Identification
- Security Monitoring
- Contactless Smart Cards
- Medical Applications

In most of these applications, the RFID systems operate in HF and UHF bands. This limits the data rate of the RFID system, and also the size of the tags is big. For tracking people and goods in the supply chain using a passive RFID system, the proposed PS algorithm would be an alternative solution, which utilizes small size tags and provides a high data rate.

The following figure shows how a tag in UHF frequency can be used to identify people. The size of this tag makes it almost uncomfortable for the patients in a hospital or for soldiers on a military field. A microwave system would solve this problem since the tags are much smaller.

Figure 33. A UHF Tag for Identification of People.

In all of the above applications, it is very important that the RFID system be reliable. This addresses the problem of data integrity, which means that collecting data from the tags must be accurate. For example, nobody wants a RFID system in a hospital or a prison which identifies the wrong person.

The proposed PS algorithm, as in most of the anticollision algorithms, promised to identify all the tagged objects in the interrogation zone given enough time, with probability equal to one. Of course, in order to succeed, the reader must somehow know the number of tags in the area.

In areas where there is a high density of tags, as with many people in a big hospital, or pallets in a supply chain consisting of many goods, the PS algorithm manages to divide the tags into smaller groups and thus identifies them easier as shown in Chapter IV.

Another solution is to use multiple readers. However, if there is not enough distance between them, one reader may interfere with the others since they are using the same frequency; a problem known in cellular communications addressed by frequency reused [18]. This is known as the *reader collision problem*, and although there are some protocols, such as the *Colorwave* anticollision algorithm proposed in [25], the problem of identifying the tags becomes more complex as with the integrity of the collected data as well.

If a passive RFID system at 2.45 GHz is used with the proposed PS algorithm, two main disadvantages/limitations occur:

- First and foremost, the effective reading range of this system is not more than 3.5 m as shown in Chapter IV, and
- A line of sight (LOS) communication between reader and tags is needed.

The first limitation in tracking goods can be solved if the pallets are forced to pass near the reader as demonstrated in Figure 33.

In this figure, the reader can be placed on top or around the check point (in green), and, therefore, the tags inside the pallets will pass near it. Notice that multiple pallets arrive at the check point at the same time, but this is not a problem when the PS algorithm is used.

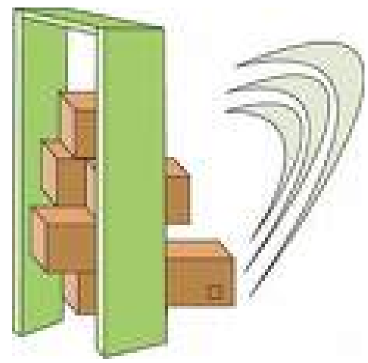


Figure 34. Identification of Goods Inside Multiple Pallets in the Supply Chain [From Ref. 26].

Also, the aforementioned procedure and design can be used to track and identify people who passed through a similar gate, for example, at an airport or on a military base.

The second limitation addressed by the proposed RFID system can be solved if two passive RFID systems are used for the pallets. The first will be the proposed RFID system with the tags placed on the pallets. The other can be a RFID system operating in UHF or HF bands, with the tags placed on each product inside the pallet. Thus, this system will first be able to track the pallet, and then each product inside.

Such a system will be more expensive, but suitable for military applications, such as for containers or pallets carrying weapons and ammunitions. For these applications, the redundancy the two RFID systems provides is more important than cost. Each time a container or pallet is shipped, it will be securely closed. It will be very easy to track it and ascertain its exact location. . The only requirement is to scan the contents at departure and arrival.

Finally, the LOS limitation might not actually be a problem. It depends on the distance of the pallets from the reader, and the reflective properties of the pallet used. Further research is necessary for a specific RFID system and application to determine if this is an actual problem.

The following section discusses how a RFID system at 2.45 GHz could also be used in military operations for *Information Warfare* (IW).

B. AN APPLICATION FOR INFORMATION WARFARE

Currently, all the aforementioned applications are dominated by passive and active RFID systems in the HF and UHF bands. It is the author's belief that in the future, higher frequencies will be very difficult to implement in areas of an already existing RFID solution and that it will increase costs to change the entire system while the benefits will almost be identical.

The main advantage of the RFID systems in the microwave ($2.45\,GHz$) band is the co-existence of other technologies such as Wireless Local Area Networks (WLAN) and Bluetooth that are using the unlicensed frequency spectrum. The Institute of Electrical and Electronics Engineers (IEEE) has already created standards for those technologies, for example, IEEE 802.11.b/g and the IEEE 802.15.1.

Furthermore, various vendors of *Remote Intelligent Communications* (RIC) products, devices similar to RFID but with many more capabilities and complexity, are working to create a "standard open protocol" for global communications at frequency $2.45\,GHz$ [27].

Thus, microwave RFID systems are the best candidates for military operations in which the above flexible and reliable technologies are used very often to provide the war fighters and decision makers with the right information at the right time.

Bluetooth and IEEE 802.11 are used very often in the exchange of information in WLAN between portable computers (Laptops) and a Personal Digital Assistant (PDA).

Figure 35 shows a British soldier with a PDA. PDA's are very common in military operations in the British army for providing networking capabilities and also

positioning capabilities by using electronic maps and GPS technology. They are used in special operations such as operations on urbanized terrain, special targets, checkpoint surveillance, border and perimeter security, and finally situational awareness.

Figure 35. A British Soldier with a PDA.

The battery life of the unit is a main limitation in networks with components in portable computers and PDA's. In [19], the author proposes a hybrid RFID tag design compatible with IEEE 802.11 and Bluetooth standards. In this design, semi-passive tags are used. For communication in a range of a few meters (up to 10m), backscatter radiation is used to exchange information between the tags and the reader, while for further distances, Bluetooth is used.

The above design is more power efficient for both the RFID system and Bluetooth and thus exceeds the battery life of the PDA. It also provides an alternative method of communication for the Bluetooth enabled device [19].

Figure 36 shows a perimeter security and situational awareness network for military operations. Such a network can be used in any kind of terrain to provide the data collection station (military vehicle on the left) with critical data in real time.

The main components in this kind of network are the war fighters/military personnel at each checkpoint who collect the data from the suspects and transmit them to the data collection station directly or via an intermediate station such as a plane. For this

transmission, a WLAN and/or Bluetooth enable PDA is used. This system's security rests on the fact that the military personnel communicating with each other use the same technology.

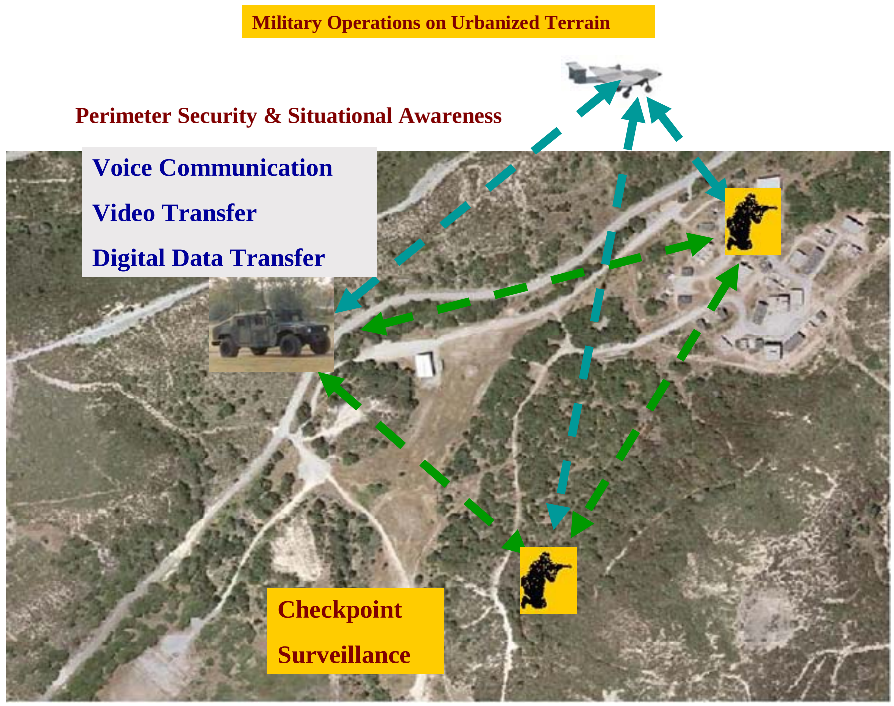


Figure 36. A Perimeter Security and Situational Awareness Network on Urbanized Terrain.

Communication between military personnel can also be achieved by using semi-passive RFID systems based on the aforementioned reasons. However, RFID tags can be also used to track every soldier participating in the operation. Thus, when a soldier approaches a checkpoint, everyone knows that this person belongs to a friendly unit. The only requirement is that the PDA's or portable computers be connected to a portable reader.

Of course, the PDA's are able to authenticate the friendly targets when communicating with each other, but tracking using the RFID tags will be able to provide a secondary method of authentication for the near approaches targets, and thus increase the overall security and reliability of the awareness system.

Finally, the soldiers, who are tagged, do not need a PDA in order to authenticate themselves at the checkpoints. Thus, by using tags, the overall cost for such a system can be significantly decreased since the cost of the tags is hundreds of times of magnitude lower than that of the PDA.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS AND FUTURE WORKS

This last chapter summarizes the results of this thesis and proposes further research in related areas of current work.

A. CONCLUSIONS

Passive RFID tags are powerless and stateless units. An important parameter for the data integrity in those systems is the currently used anticollision protocol. A common anticollision protocol in RFID systems is the Framed Slotted Aloha and variations of FSA.

The performance of a FSA algorithm using either the throughput or the average time delay as a measure of efficiency shows that a high correlation exists between the number of tags in the interrogation zone and the frame size which the reader uses.

A high density of tags near the reader increases the frame size required from the reader in order for the system to operate in the area of maximum theoretical throughput. However, always using a large frame size introduces more delays in the system, and thus decreases the performance of the RFID system. For this reason, DFSA with a variable frame size in the beginning of each cycle performs better. Simulations proved that when using DFSA, the system is more stable and needs less time to identify all the tags in the interrogation zone.

Microwave RFID systems experience the largest path loss than any other RFID system. Tags using current technology demonstrated that the maximum LOS distance that a passive system can achieve is equal to $3.5\ m$.

Using the ISO standards and the simplest backscatter modulation (ASK), it was proven that the probability for a tag to transmit its data with an error is quite high, and for the optimal frame length of $96\ bits$, the signal-to-noise ratio must be above 12 dB in order to be very low (almost 10^{-3} and lower).

The use of capture effect in RFID systems can be very beneficial, and for the typical reader's sensitivity of 6 dB, it can improve the maximum theoretical throughput and increase it to $46\,\%$.

This thesis proposes a variation of the FSA called the Progressing Scanning algorithm. PS promises to improve the performance of the FSA when the number of tags in the area is too high by dividing the tags into groups and dealing with each group individually.

The parameters that control the performance of the PS algorithm are the minimum transmitted power level from the reader, the frame size, and finally the step of increasing the power in each cycle. Different values cause the PS algorithm to perform differently. Generally, the PS algorithm is better than FSA when the number of tags in the area is over 800. Smaller steps increase the performance of the PS algorithm for systems with high density of tag's in the area.

Furthermore, higher frame sizes correspond to a higher initial average delay, but can also handle more tags due to collisions. The most important conclusion for the performance of the proposed algorithm is that it can very simply provide a high degree of data integrity in the RFID system, even with the use of small frame sizes, while FSA cannot.

Last but not least, this thesis proposes the use of a semi-passive microwave RFID system with protocol compatible with IEEE 802.11 and IEEE 802.15 for power efficiency and also able to identify and track friendly forces.

B. FUTURE WORKS

1. Effect of Multipath in the Performance of the RFID Channel

Microwave RFID systems need LOS communication between the reader and tags. This thesis has not evaluated the performance of a typical RFID system with multipath fading. It would be interesting to see how this performance would change in a multipath Ricean fading channel, and then compare that with the results of this thesis.

2. Distribution of Tags in the Interrogation Zone

The simulation of the performance for the PS algorithm was done by assuming that the distance of the tags inside the interrogation zone is uniformly distributed. This normally occurs in practice (scanning goods in a cart or passing them beneath a checkpoint), but it would be helpful to compare the PS algorithm to different distributions, such as *Gaussian.*

3. Dynamic Framed PS Algorithm

Further research is necessary to simulate the PS algorithm to calculate the optimal frame size and dynamic change at the beginning of each new cycle. The optimal frame size must be equal to the estimated number of tags in the previous cycle. The number of tags can be estimated by one of the formulas given in Chapter IV.

Also, it would be interesting to compare the dynamic PS algorithm with DFSA to verify if the results are similar to those of this thesis which compare FSA to the PS algorithm. Most probably, a dynamic PS algorithm would be superior to DFSA for an environment with a high density of tags.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] Manish Bhuptani and Shahram Moradpour, *RFID Field Guide, Deploying Radio Frequency Identification Systems*, Sun Microsystems, 2005.

[2] Klaus Finkenzeller, *RFID Handbook, Fundamentals and Applications in Contactless Smart Cards and Identification*, Wiley, Second Edition, 2004.

[3] Sandip Lahiri, *RFID Sourceboo*k, IBM Press, 2005.

[4] Simson Garfinkel and Beth Rosenberg, *RFID Applications, Security, and Privacy,* Wesley, New Jersey, 2005.

[5] William Stallings, *Data and Computer Communications,* Pearson/Prentice Hall, Seventh Edition, New Jersey, 2004.

[6] EPC Radio-Frequency Identity Protocols Generation 2 Identity Tag (Class 1): Protocol for Communications at 860 MHz-960 MHz. EPC Global Hardware Action Group (HAG), EPC Identity Tag (Class 1) Generation 2, Last-call Working Draft Version 1.0.2, 2003-11-24.

[7] Simon Haykin, *An Introduction to Analog and Digital Communications*, Wiley, 1989.

[8] Index of site on Apache/1.3.33 Server at delo.dcs.fmph.uniba.sk Port 80, http://delo.dcs.fmph.uniba.sk/, May 18, 2006, www.delo.dcs.fmph.uniba.sk/2inf/store/distrsys/i2cn_html/ch2s4p1.htm, last accessed on February 6, 2006.

[9] LinuxDevices.com, *Device Profile: ThingMagic Mercury4 RFID Reader*, August 19, 2005, http://www.linuxdevices.com/articles/AT9437876354.html, last accessed on February 6, 2006.

[10] EPCglobal US, http://www.epcglobalus.org, 2006, last accessed on February 6, 2006.

[11] Jae-Ryong Cha and Jae – Hyun Kim, *Novel Anti-Collision Algorithms for Fast Object Identification in RFID System,* IEEE ,Computer Society, Proceedings of the 2005 11th International Conference on Parallel and Distributed Systems (ICPADS), Volume 2, pp. 63-67, July 20-22, 2005.

[12] Frits C. Schoute, *Dynamic Frame Length ALOHA*, IEEE Transactions on Communications, Vol. 31, issue 4, pp. 565-568, April 1983.

[13] Harald Vogt, *Efficient Object Identification with Passive RFID Tags*, In International Conference on Pervasive Computing, pp. 98-113, Pervasive2002, Springer-Verlag, April 2002.

[14] Harald Vogt, *Multiple Object Identification with Passive RFID Tags,* IEEE International Conference on Systems, Man and Cybernetics (SMC '02), Volume 3, pp. 4-9, October 2002.

[15] Peyton Z. Peebles, JR, *Probability, Random Variables and Random Signals Principles,* McGraw Hill, Fourth Edition, 2001.

[16] Su-Ryun Lee, Sung-Don Joo and Chae-Woo Lee, *An Enhanced Dynamic Framed Slotted ALOHA Algorithm for RFID Tag Identification*, IEEE, Computer Society, Proceedings of the Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous 2005), pp. 166-172, July 17-21, 2005.

[17] ISO/IEC, *18000 Part 4: Parameters for Air Interface Communications at 2.45 GHz,* ISO, 2004.

[18] Theodore S. Rappaport, *Wireless Communications- Principles and Practices*, Prentice Hall, Second Edition, New Jersey, 2002.

[19] Raj Bridgelall, *Bluetooth/802.11 Protocol Adaptation for RFID Tags, Symbol Technologies*, RFDESIGN, July 1, 2002.

[20] Giuseppe De Vita and Giuseppe Iannaccone, *Design Criteria for the RF Section of UHF and Microwave Passive RFID Transponders*, IEEE Transactions on Microwave Theory and Techniques, vol. 53, no. 9, pp. 2978-2990, September 2005.

[21] Pete Sorrells, *Passive RFID Basics,* AN680, DS00680B, pp. 1-5, Microchip Technology Inc., 1998.

[22] Feng Zhou, Chunhong Chen, Dawei Jim, Chenling Huang and Hao Min, *Evaluation and Optimizing Power Consumption of Anticollision Protocols for Applications in RFID Systems,* pp. 357-362, ISLPED'04, Newport Beach, California, USA, August 9-11, 2004.

[23] Flaminio Borgonovo and Michele Zorzi, *Slotted ALOHA and CDPA: A Comparison of Channel Access,* pp. 43-51, J.C. Baltzer AG, Science Publishers, Wireless Networks 3, 1997.

[24] Steven Shepard, *RFID, Radio Frequency Identification,* McGraw-Hill, First Edition, Fairfield, 2005.

[25] James Waldrop, Daniel W. Engels, Sanjay E. Sarma, *Colorwave: An Anticollision Algorithm for the Reader Collision Problem,* Communications, 2003. ICC '03. IEEE International Conference on Volume 2, May 11-15, 2003. pp. 1206 – 1210.

[26] Raco Industries, LLC, http://www.racoindustries.com/intellitrack_slap_and_ship.htm, last accessed on June 31, 2006.

[27] John R. Tuttle, *Traditional and Emerging Technologies and Applications in the Radio Frequency Identification (RFID) Industry,* volume I-2, pp. 5-8, IEEE RFICS, 1997.

[28] Dynasys Technologies, Inc., 2005, http://rfidusa.com/superstore/product_info.php?cPath=34&products_id=521, last accessed on August 5, 2006.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Fort Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Chairman ,Code EC/Ko
   Department of Electrical and Computing Engineering
   Naval Postgraduate School
   Monterey, California

4. Chairman ,Code IS/Bo
   Department of Information Sciences
   Naval Postgraduate School
   Monterey, California

5. Professor Weilian Su, Code EC/Su
   Department of Electrical and Computing Engineering
   Naval Postgraduate School
   Monterey, California

6. Professor Tri T. Ha, Code EC/Ha
   Department of Electrical and Computing Engineering
   Naval Postgraduate School
   Monterey, California

7. Embassy of Greece, Naval Attaché
   Washington, DC

8. Nikolaos Alchazidis,
   Mpasiakou 8
   Thiva, GREECE
   T.K. 32200